EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	4	"672811".ap.	US-PGPUB; USPAT	OR	OFF	2007/10/11 21:12
L2	1476	(380/28).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 21:49
L3	1157	2 and @ay <="2003"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 21:49
L4	11	3 and (factor) and (equation) and (derivative)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/10/11 22:09
L5	0	(derivative) same ("not" determin$4 factor)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/10/11 21:54
L6	0	false derivate	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	OFF	2007/10/11 21:54
L7	0	false derivative value	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/10/11 21:54

EAST Search History

L8	0	(derivative value) same ("not" determin$4 factor)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/10/11 21:55
L9	0	(derivative value) same ("not" with factor)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/10/11 21:55
L10	121	(380/263).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 21:55
L11	87	10 and @ay<="2003"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 21:56
L12	5	11 and (factor) and (equation) and (derivative)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/10/11 21:56
L13	1339	(380/30).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 21:57
L14	1179	13 and @ay<="2003"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 21:57

EAST Search History

L15	7	14 and (factor) and (equation) and (derivative)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/10/11 21:57
L16	806	(380/46).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 21:57
L17	720	16 and @ay <="2003"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 21:57
L18	8	17 and (factor) and (equation) and (derivative)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/10/11 21:58
L19	350	(380/42).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 21:59
L20	303	19 and @ay<="2003"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 21:59
L21	1	20 and (factor) and (equation) and (derivative)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/10/11 22:02

EAST Search History

L22	261	(380/45).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 22:02
L23	249	22 and @ay <="2003"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 22:02
L24	1	23 and (factor) and (equation) and (derivative)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/10/11 22:03
L25	395	(713/180).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 22:03
L26	352	25 and @ay<="2003"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 22:03
L27	1	26 and (factor) and (equation) and (derivative)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/10/11 22:04
L28	2015	(713/168).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 22:04

EAST Search History

L29	1476	28 and @ay<="2003"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 22:04
L30	6	29 and (factor) and (equation) and (derivative)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/10/11 22:05
L31	281	(708/491).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 22:05
L32	257	31 and @ay<="2003"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 22:06
L33	6	32 and (factor) and (equation) and (derivative)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/10/11 22:07
L34	308	(708/492).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 22:08
L35	265	34 and @ay<="2003"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 22:08

EAST Search History

L36	5	35 and (factor) and (equation) and (derivative)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/10/11 22:08
L37	5410	(709/217).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 22:09
L38	4306	37 and @ay<="2003"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 22:09
L39	12	38 and (factor) and (equation) and (derivative)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/10/11 22:09
L40	0	((encrypt$4) and (decrypt$4) and (original string) and (defin$4 set of factors) and (encrypt$4 equation) and (map$4) and (a set of derivative equations) and (generat$4 derivative values) and (stor$4 encrypted string and derivative values) and (provid$4 false derivatives cannot be used to determine a given factor) and (stor$4 false derivative values with the generated derivative values) and (us$4 a set of factor decryption equatins to map) and (decrypt$4 the encrypted string) and (decryption equation) and (factor mapped through the set of factor decryption equation) and (presence) and (false derivative values with the generated derivative values) and (prevent$4) and (use with the factor decryption equation to derive the factors in the set of facotrs)).clm.	US-PGPUB; USPAT	ADJ	ON	2007/10/11 22:47

EAST Search History

L41	6	Cheung-tom-thuan.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/10/11 22:48
S1	2	"672811".ap.	USPAT	OR	OFF	2007/03/02 10:44
S2	3	"672811".ap.	US-PGPUB; USPAT	OR	OFF	2006/12/01 16:29
S3	194	("20050069127" "4893338" "5857025" "6049608" "6078665" "20020154769" "20040086117" "5666419" "6259790" "6317769" "20020055962" "20030081769" "20030215089" "20050195973" "6058189" "4306111" "5675653" "4969190" "5727064" "5982900" "6128386" "6330674" "6449473" "7133522" "20030007639" "20030059040" "20030118185" "20030210781" "4423287" "4578530" "5313521" "5214698" "5953419" "5265164" "5517567" "5796830" "5987133" "6003136" "6009175" "6055639" "6175920" "6230002" "5224166" "5365589" "5412729" "5481613" "5539827" "5694470" "5787175" "5799086" "5815573" "5841865" "5850451" "5857022" "5864683" "5872849" "5917910" "5920630" "5937066" "5956408" "6009177" "6052469" "6061454" "6061454" "6072876" "6122742" "6185316" "6202150" "6249866" "4295039" "4302810" "4438824" "4500750" "4817140" "4825050" "4881263" "4924513" "4972472" "5001754" "5010573" "5200999" "5208853" "5222140" "5228084" "5295188" "5345506" "5365588" "5384850" "5420866" "5425103" "5434920" "5448638" "5455861" "5495533" "5541994" "5594798" "5604801" "5615268" "5619576").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/12/01 16:54

EAST Search History

S4	24	("5677952"|"5751811"|"5781632"|"5805712"|"5987133"|"6002769"|"6226618"|"6230272"|"6324287"|"6345288"|"6351813"|"6389541").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/12/01 16:56
S5	1	"5862325".pn.	USPAT	OR	OFF	2006/12/01 16:55
S6	1	"5915024".pn.	USPAT	OR	OFF	2006/12/01 16:55
S7	1	"6226383".pn.	USPAT	OR	OFF	2006/12/01 16:55
S8	40	(derivative equation) and (factor) and (encrypt$4) and (decrypt$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/12/04 20:32
S9	1287	(380/28).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/12/04 20:33
S10	2	S9 and S8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/12/04 20:33
S11	44	("4074066" | "4238854" | "4319079" | "4593353" | "4734796" | "4888798" | "4907274" | "5003597" | "5212729" | "5239581" | "5454039").PN. OR ("5677952"). URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2006/12/06 13:36
S12	2583	(password) and (deriv$5) and (factor) and (encryp$4) and (decrypt$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 13:57
S13	934	(password) and (deriv$5) and (factor) and (encryp$4) and (decrypt$4)	USPAT	OR	ON	2006/12/07 13:58

EAST Search History

S14	5	(password) same (deriv$5) same (factor) same (encryp$4) same (decrypt$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 16:00
S15	1	"6845453".pn.	USPAT	OR	OFF	2006/12/07 14:01
S16	13	("5280527" | "5499297" | "5805719" | "5907597" | "6035398" | "6035406" | "6307955" | "6317834" | "6332193" | "6385318" | "6553494").PN. OR ("6845453"). URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2006/12/07 14:05
S17	1	(password) same (derivative) same (factor) same (encryp$4) same (decrypt$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 15:26
S18	900	(password) and (derivative) and (factor) and (encryp$4) and (decrypt$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 15:26
S19	341	(password) and (derivative) and (factor) and (encryp$4) and (decrypt$4)	USPAT	OR	ON	2006/12/07 15:27
S20	1274	(380/28).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; JPO; DERWENT; IBM_TDB	OR	OFF	2006/12/07 15:27
S21	6	S18 and S20	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/12/07 15:31

EAST Search History

S22	2390	factor same encryp$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 15:32
S23	956	factor same encryp$4	USPAT	OR	ON	2006/12/07 15:32
S24	360	factor with encryp$4	USPAT	OR	ON	2006/12/07 15:32
S25	1	"6075865".pn.	USPAT	OR	OFF	2006/12/07 16:00
S26	3	("5375169" | "5787173" | "5835597").PN. OR ("6075865"). URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2006/12/07 16:07
S27	1	"5048086".pn.	USPAT	OR	OFF	2006/12/08 09:38
S28	1	"20020176377".pn.	US-PGPUB; USPAT	OR	OFF	2007/03/02 10:45
S29	3	"672811".ap.	US-PGPUB; USPAT	OR	OFF	2007/05/15 09:58
S30	3	"672811".ap.	US-PGPUB; USPAT	OR	OFF	2007/05/23 11:23
S31	1	"5048086".pn.	US-PGPUB; USPAT	OR	OFF	2007/05/23 11:23
S32	62	("5007087").PN. OR ("5048086"). URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2007/05/23 11:34
S33	0	generat$4 with (random number) with ("not") with chaos	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/05/23 11:36
S34	0	("not") with chaos	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/05/23 11:35
S35	1	("not") same chaos	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/05/23 11:35

EAST Search History

S36	0	generat$4 same (random number) same ("not") same chaos	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/05/23 11:36
S37	0	(random number) same ("not") same chaos	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/05/23 11:37
S38	10	chaos equation	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/05/23 11:44
S39	0	(encryp$4) with ("not") with (base$2) with (chao$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/05/23 11:41
S40	0	(encryp$4) same ("not") same (base$2) same (chao$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/05/23 11:41
S41	4282	("not" or "no" or "unlike") same (chaos)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/05/23 11:45
S42	2265	("not" or "no" or "unlike") with (chaos)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/05/23 11:45

EAST Search History

S43	2256	("not" or "no") with (chaos)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/05/23 11:48
S44	168	(without) with (chaos)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/05/23 11:45
S45	154	S42 and (encrypt$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/23 11:47
S46	168	("not" or "without") with (chaos)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/05/23 11:49
S47	17	S46 and (encrypt$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/05/23 12:02
S48	0	"672811".pn.	US-PGPUB; USPAT	OR	OFF	2007/05/23 15:16
S49	3	"672811".ap.	US-PGPUB; USPAT	OR	OFF	2007/05/23 15:16
S50	1	"5677952".pn.	USPAT	OR	OFF	2007/05/24 10:03
S51	1295	(380/28).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/05/24 12:16
S52	0	("672811.ap.").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2007/10/06 20:43
S53	4	"672811".ap.	US-PGPUB; USPAT	OR	OFF	2007/10/06 20:43

EIC Comprehensive search

```
File 696:DIALOG Telecom. Newsletters 1995-2007/Oct 10
         (c) 2007 Dialog
File   9:Business & Industry(R) Jul/1994-2007/Oct 03
         (c) 2007  The Gale Group
File  15:ABI/Inform(R) 1971-2007/Oct 11
         (c) 2007 ProQuest Info&Learning
File  98:General Sci Abs 1984-2007/Sep
         (c) 2007 The HW Wilson Co.
File 484:Periodical Abs Plustext 1986-2007/Oct W1
         (c) 2007 ProQuest
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 613:PR Newswire 1999-2007/Oct 11
         (c) 2007 PR Newswire Association Inc
File 635:Business Dateline(R) 1985-2007/Oct 11
         (c) 2007 ProQuest Info&Learning
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 610:Business Wire 1999-2007/Oct 11
         (c) 2007 Business Wire.
File 369:New Scientist 1994-2007/Sep W1
         (c) 2007 Reed Business Information Ltd.
File 370:Science 1996-1999/Jul W3
         (c) 1999 AAAS
File  16:Gale Group PROMT(R) 1990-2007/Oct 09
         (c) 2007 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2007/Sep 26
         (c) 2007 The Gale group
File 148:Gale Group Trade & Industry DB 1976-2007/Oct 04
         (c)2007 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2007/Oct 04
         (c) 2007 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2007/Oct 05
         (c) 2007 The Gale Group
File 624:McGraw-Hill Publications 1985-2007/Oct 10
         (c) 2007 McGraw-Hill Co. Inc
File 634:San Jose Mercury  Jun 1985-2007/Oct 10
         (c) 2007 San Jose Mercury News
File 636:Gale Group Newsletter DB(TM) 1987-2007/Oct 09
         (c) 2007 The Gale Group
File 647:CMP  Computer Fulltext 1988-2007/Sep W5
         (c) 2007 CMP Media, LLC
File 674:Computer News Fulltext 1989-2006/Sep W1
         (c) 2006 IDG Communications
File 239:Mathsci 1940-2007/Oct
         (c) 2007 American Mathematical Society

Set     Items   Description
S1    1367162   FALSE OR INVALID OR NULL OR PSUEDO OR PSEUDO OR RANDOM OR -
              RAND OR CHAFF OR SEMIRANDOM OR PSUEDORAND? OR PSEUDORAND? OR -
              DUMMY OR NONCE? ? OR DECOY?
S2     196815   SHILL??  OR SPOOF?? OR PHONEY? ? OR PHONY? ? OR PHONIE? ? -
              OR FAKE? ? OR SHAM OR SHAMS
S3      31249   S1:S2(1W)(VALUE OR VALUES OR NUMBER? ? OR NUMERAL? ? OR NU-
              MERIC?? OR ALPHANUMERIC? OR QUANTITY? ? OR QUANTITIES OR CHAR-
              ACTER? ? OR BIT OR BITS OR DATA OR DATUM? ?)
S4      82185   S1:S2(1W)(DIGIT? ? OR SIGNAL? ? OR PULSE OR PULSES OR INTE-
              GER? ? OR STRING OR STRINGS OR SUBSTRING? ? OR SEQUENCE OR SE-
              QUENCES OR SUBSEQUENCE? ? OR NOISE OR VARIABLE? ?)
S5   29552231   USED OR USE OR USING OR USAGE? ? OR EMPLOY? OR UTILIS??? OR
               UTILISATION? ? OR UTILIZ??? OR UTILIZATION? ?
```

```
S6     489797   NONEMPLOY? OR UNEMPLOY? OR NONUTILIS? OR NONUTILIZ? OR UNU-
             TILIS? OR UNUTILIZ?
S7     142283   NONUSE? OR NONUSING OR NONUSAGE? OR UNUSE? OR UNUSING OR U-
             NUSAGE? OR DISUSE? ? OR DISUSING OR DISUSAGE?
S8    1035688   ('NOT' OR WITHOUT OR NEVER OR CANNOT OR T) (1W)S5
S9      18436   (NON OR UN OR DIS)()S5
S10      1442   S3:S4(5N)(OMIT? OR OMISSION? ? OR EXCLUD? OR EXCLUSION?)
S11       163   S3:S4(5N)S8:S9
S12    261023   DECRYPT? OR UNCRYPT? OR UNENCRYPT? OR DECOD??? OR UNENCOD?-
             ?? OR UNCOD??? OR UNENCRYPT? OR UNENCIPHER? OR UNENCYPHER? OR
             DECIPHER? OR DECYPHER?
S13     99025   UNSCRAMBL? OR DESCRAMBL? OR UNCIPHER? OR UNCYPHER? OR DECO-
             MPRESS? OR DEPACK? OR UNPACK? OR UNCOMPRESS? OR DECOMPACT? OR
             UNCOMPACT?
S14       214   S3:S4(5N)S6:S7
S15         3   (S10:S11 OR S14)(50N)S12:S13
S16         1   RD  (unique items)
S17       211   AU=(CHEUNG T? OR CHEUNG, T?)
S18         0   S17 AND (S10:S11 OR S14)
S19         0   S17 AND S3:S4
S20         7   (S10:S11 OR S14)(100N)S12:S13
S21         4   S20 NOT S15
S22         2   RD  (unique items)

 22/3,K/1     (Item 1 from file: 484)
DIALOG(R)File 484:Periodical Abs Plustext
(c) 2007 ProQuest. All rts. reserv.

01988726   (USE FORMAT 7 OR 9 FOR FULLTEXT)
Prying open the Clipper lock
Anonymous
Science News (GSCN), v145 n24, p383, p.1
 Jun 11, 1994
 ISSN:  0036-8423       JOURNAL CODE:  GSCN
 DOCUMENT TYPE:  News
 LANGUAGE:  English            RECORD TYPE:  Fulltext; Abstract
WORD COUNT:  331        LENGTH: Short  (1-9 col inches)

TEXT:
...     it by taking advantage of the fact that to obtain the right master
key to  decipher  a message, the government has to find out the encryption
chip's serial number. This...

...legitimate. It then substitutes a bogus LEAF, which has the same
checksum but includes a  fake  serial  number  that can' t  be  used  by
the government. Officials of the National Security Agency concede the
existence of the flaw...


 22/3,K/2     (Item 1 from file: 47)              full-text of article is
DIALOG(R)File  47:Gale Group Magazine DB(TM)            included at the end
of this
(c) 2007 The Gale group. All rts. reserv.                    printout.

02368408     SUPPLIER NUMBER: 02743601    (USE FORMAT 7 OR 9 FOR FULL TEXT)
Basic cryptography: SBOEPN DJQIFST.
Wheeler, Daniel D.; Perri, Elisheva
Creative Computing, v9, p178(4)
May, 1983
ISSN: 0097-8140      LANGUAGE: ENGLISH      RECORD TYPE: FULLTEXT
WORD COUNT:   2134    LINE COUNT:  00156

...     130 is included only to make a complete statement; the value stored
in X is  never  used .
```

Setting the random number seed on the IBM PC is a trivial process, as the RANDOMIZE function allows automation...also be noted that messages for enciphering must be input in upper case, for proper decoding . The rest of the program follows other Microsoft versions closely.
There is no instruction to...

22/9/2 (Item 1 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)

02368408 SUPPLIER NUMBER: 02743601 (THIS IS THE FULL TEXT)
Basic cryptography: SBOEPN DJQIFST.
Wheeler, Daniel D.; Perri, Elisheva
Creative Computing, v9, p178(4)
May, 1983
ISSN: 0097-8140 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 2134 LINE COUNT: 00156

TEXT:
Basic Cryptography: SBOEPN DJQUIFST

The personal computer is a powerful tool for cryptography. With a bit of simple programming you can encipher secret messages to your friends so securely that it would take the efforts of a mathematical cryptographer to unravel the system. But with the proper keyword a friend can use his computer to decipher and read your message.

There have been several programs for simple cryptography published in the major computer magazines. Some of these programs, unfortunately, have used very weak systems for enciphering the messages. Anyone with a little knowledge of cryptanalytic techniques could break the system and read the messages without knowing the keyword.

This article explains the principles of computer cryptography and demonstrates the use of the Basic random number function for enciphering messages. Versions of the program are included for the Apple II, the TRS-80 Models I and III, IBM PC, and the Atari 400 and 800.

Cryptography by Addition

Letters are represented in computers as numbers. This makes it easy to use the arithmetic operations of Basic to transform the letters. The simplest system is just to add a constant number to the character code for each letter. If the result is too large, subtract the number of characters being used so that the result is again a valid character code. Suppose, for instance, that you want to use three as the constant and that your messages consist of only capital letters. Then each letter in the message will come out as the letter three letters further on in the alphabet. The letter A (ASCII code 65) will appear as D (ASCII code 68), B(66) becomes E(69), and so forth. A the end of the alphabet, X (88) becomes the ASCII code 91. But 90 is Z and 91 is beyond the end of the alphabet. So 26 (the number of characters we are using) is subtracted from 91 to produce 65. Thus X wraps around to the beginning of the alphabet and becomes A.

The Basic statements necessary to do this are quite simple. If the letter to be transformed is stored in the string A$, you can do it with:

```
100 = ASC(A$ )
110 X = X 3
120 IF > 90 THEN = - 26
130 A$ = CHR$ (X)
```

The ASC(A$) function converts the character to a numeric variable so that the arithmetic can be done in the next two statements. The CHR$ (X) function converts the numeric result back into a string.

To decipher the message, change lines 110 and 120 to:

```
110 X = X - 3
120 IF < 65 THEN = 26
```

This system is called a Caesar cipher because Julius Caesar is said to have used it. It may have fooled the Gauls, but now any bright elementary school student (maybe with a hint) can break the system. Part of

the title of this article is in the Caesar cipher, but not with an offset of three.

Better Systems

The weakness of the system comes from the use of the constant. There are only 25 possible constants to try and once you figure it out it is easy to decipher the whole message. You can improve the system by changing the offset for each character. You might try adding one to the offset each time you encipher a character and then subtracting 26 from the constant whenever it gets too large. This will produce a cipher that is much more difficult to break.

There are many possible schemes for changing the offset. Any scheme will work to make the cipher more difficult to break. But if the scheme is simple (like adding one) and repeats at fairly short, regular intervals, then it is not very difficult to figure out the pattern and break the cipher. A smart high school student could do it.

What you need is an irregular pattern that doesn't repeat within the length of the messages you are interested in sending. The random number function in Basic provides a very irregular series of numbers. They do repeat eventually, but the cycle is much longer than any messages you will ever send on your computer.

If the random number function were truly random, it would not be useful for our purpose. Once you have enciphered a message, your recipient must be able to generate the same sequence of numbers to decipher the message. Fortunately, most versions of Basic provide some way to "seed' the random function so that it generates the same sequence of numbers.

In Applesoft, for instance, calling the random number function with a negative argument, such as RND (-99), seeds the generator to start at a definite place in the sequence. If you agree beforehand on a number to use as the seed, your friend will be able to decipher your message by generating the same sequence of numbers to use as offsets.

Demonstration Programs

Listings 1, 2, 3, and 4 show programs to demonstrate these techniques for four popular microcomputers. Each of the programs enciphers or deciphers a one-line secret message. Instead of enciphering just the letters of the message, these programs encipher everything: letters, numbers, punctuation marks and even spaces. (The ASCII code for the space is 32. It is just as much a character as any of the others. You must be especially careful in typing the enciphered message to get all the spaces exactly right.)

The program lines in the 100's initialize the random number generator. For the Apple this is simply a matter of calling the random number generator with a negative argument. The variable X in line 130 is included only to make a complete statement; the value stored in X is never used.

Setting the random number seed on the IBM PC is a trivial process, as the RANDOMIZE function allows automation of the seed generation. By omitting an argument in the RANDOMIZE command in line 110, the PC will return with the default input statement, Random Number Seed (-32768 to 32767)? You may then input your cipher base value. The message is input with an INKEY command, so backspacing is impossible. It should also be noted that messages for enciphering must be input in upper case, for proper decoding. The rest of the program follows other Microsoft versions closely.

There is no instruction to initialize the RND() function in TRS-80 Level II Basic, but it can be done with POKEs into memory. Lines 130-150 show how to do it. POKEs can only be done with numbers smaller than 256. The instructions in lines 140 and 150 break the larger seed (stored in N) into two parts, each less than 256.

We couldn't figure out how to seed the RND() function in Atari Basic, so we'll show you how to write your own random function. The initial seed must be a decimal fraction between zero and one. In lines 110-140 the program gets a number and then divides by 100,000 to make it a fraction.

The lines in the 200's allow you to select whether the message will be enciphered (by adding the random numbers) or deciphered (by subtracting

the random numbers).

The next section of the program (300's) allows you to enter your message. For the Atari this is a straight-forward INPUT statement. Then the loop in lines 340-360 converts the characters to the numeric (ASCII code) values and stores them in the array IN(). But neither the Apple nor the TRS-80 allows commas within input strings. The comma is used to separate multiple items in the input. Since we wanted to include the comma as an allowable character we used the single character input commands. These car GET on the Apple and INKEY$ on the TRS-80. The program loop starting at line 330 accepts single characters, converts them to numeric form, and stores the ASCII codes in the integer array IN%().

When the message is completely entered, the program goes to the section either to encipher (400's) or decipher (500's) the message. There are 59 possible characters from "space' (ASCII 32) to Z (ASCII 90). To encipher the message we should add a random integer up to 59 to each of the character codes. This is easy on the TRS-80.

The RND() function with arguments larger than one returns integers in the range from one to the value of the argument. Thus RND(59) returns integers from 1 to 59. These are added to the character codes in line 420. Line 430 subtracts 59 if the result is out of the allowable range. Line 430 converts the numeric code to a character and prints it. The loop in lines 410-450 repeats this for each character in the message.

The Apple RND() function returns decimal fractions between zero and one. To convert to a random integer we multiply by 59 and use the INT() function to make the result an integer. This appears in line 420. The rest of the loop is exactly the same as for the TRS-80.

In the Atari version we don't use the built-in RND() function. We store the seed for our own random function in the variable N. To get each successive random number we multiply N by 997 and take the fractional part of the result to use as the random number and to store in N for generating the next number. Line 420 does this by calculating 997*N and subtracting the integer part to leave the fractional part. Then N is used in line 430 as a random number in the range zero to one, just as in the Apple version.

The section to decipher the message (lines in the 500's) is exactly the same as the enciphering section except that the additions and subtractions are reversed. It will restore an enciphered message to its original form.

Extending the Demonstration Programs

These demonstration programs are not intended for practical use. They can, however, be extended to meet your cryptographic needs. You will certainly want to put in a loop so that your messages can be more than one line long. You will probably want the output written on disk or cassette so the person receiving your message won't have to type the random-appearing enciphered text. Output to a modem for telephone communication is another possibility. Your imagination is the only limit.

Breaking Random Ciphers

You might think that the ciphers based on random number generators would be impossible to break. After all, the enciphered message looks just like a random sequence of characters. There is no pattern to give clues to the content of the message. During World War II the Germans were confident that their machine cipher was secure. But first the Poles and then the British were able to break it. Churchill was reading Hitler's war dispatches--sometimes even before they got to Hitler.

The method requires that the cryptographer be able to guess a word in the message. For instance, if the message looks as though it was intended as a letter, it is likely to begin "Dear . . .' The cryptographer subtracts the ASCII codes for "Dear' from the message to recover part of the sequence of the random number generator. It is possible to figure out from a few numbers where the random number generator is in its sequence. Then it is a simple matter to generate the entire sequence and decipher the whole message. If the first attempt doesn't work, the cryptographer tries other probable words in all possible positions in the message.

There are techniques for enciphering messages that are resistant to the probable word method. If you have a serious security problem you should

get a commercially available, tested system. But for most personal computer users the ciphers based on the Basic random function provide a reasonable degree of security. Unless your lover's spouse is a mathematician, you'll be able to keep your letters secret with Basic random ciphers.

Table: Listing 1. Apple II version of the random cipher program.
Table: Listing 2. TRS-80 version of the random cipher program.
Table: Listing 3. Atari version of the random cipher program.
Table: Listing 4. IBM PC version of the random cipher program.
Table: Sample Run.

DESCRIPTORS: cryptography--Equipment and supplies; Ciphers--Computer programs
FILE SEGMENT: MI File 47

File 348:EUROPEAN PATENTS 1978-2007/ 200739
(c) 2007 European Patent Office
File 349:PCT FULLTEXT 1979-2007/UB=20070927UT=20070920
(c) 2007 WIPO/Thomson

Set	Items	Description
S1	477716	FALSE OR INVALID OR NULL OR PSUEDO OR PSEUDO OR RANDOM OR -RAND OR CHAFF OR SEMIRANDOM OR PSUEDORAND? OR PSEUDORAND? OR -DUMMY OR NONCE? ? OR DECOY?
S2	13399	SHILL?? OR SPOOF?? OR PHONEY? ? OR PHONY? ? OR PHONIE? ? -OR FAKE? ? OR SHAM OR SHAMS
S3	34577	S1:S2(1W)(VALUE OR VALUES OR NUMBER? ? OR NUMERAL? ? OR NU-MERIC?? OR ALPHANUMERIC? OR QUANTITY? ? OR QUANTITIES OR CHAR-ACTER? ? OR BIT OR BITS OR DATA OR DATUM? ?)
S4	31600	S1:S2(1W)(DIGIT? ? OR SIGNAL? ? OR PULSE OR PULSES OR INTE-GER? ? OR STRING OR STRINGS OR SUBSTRING? ? OR SEQUENCE OR SE-QUENCES OR SUBSEQUENCE? ? OR NOISE OR VARIABLE? ?)
S5	2256842	USED OR USE OR USING OR USAGE? ? OR EMPLOY? OR UTILIS??? OR UTILISATION? ? OR UTILIZ??? OR UTILIZATION? ?
S6	1304	NONEMPLOY? OR UNEMPLOY? OR NONUTILIS? OR NONUTILIZ? OR UNU-TILIS? OR UNUTILIZ?
S7	40445	NONUSE? OR NONUSING OR NONUSAGE? OR UNUSE? OR UNUSING OR U-NUSAGE? OR DISUSE? ? OR DISUSING OR DISUSAGE?
S8	397884	('NOT' OR WITHOUT OR NEVER OR CANNOT OR T) (1W)S5
S9	24360	(NON OR UN OR DIS)()S5
S10	376	S3:S4(5N)(OMIT? OR OMISSION? ? OR EXCLUD? OR EXCLUSION?)
S11	409	S3:S4(5N)S8:S9
S12	146747	DECRYPT? OR UNCRYPT? OR UNENCRYPT? OR DECOD??? OR UNENCOD?-?? OR UNCOD??? OR UNENCRYPT? OR UNENCIPHER? OR UNENCYPHER? OR DECIPHER? OR DECYPHER?
S13	45013	UNSCRAMBL? OR DESCRAMBL? OR UNCIPHER? OR UNCYPHER? OR DECO-MPRESS? OR DEPACK? OR UNPACK? OR UNCOMPRESS? OR DECOMPACT? OR UNCOMPACT?
S14	119	S3:S4(5N)S6:S7
S15	77	(S10:S11 OR S14)(50N)S12:S13
S16	56	S15 AND PY=1963:2003
S17	31	S15 AND (AC=US OR AC=US/PR) AND AY=1978:2003
S18	61	S16:S17
S19	61	IDPAT (sorted in duplicate/non-duplicate order)
S20	61	IDPAT (primary/non-duplicate records only)

? t20/5,k/7,16,19,21,27,31,36,38-39,50-51,61

20/5,K/7 (Item 7 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01439227
Method, apparatus and program for quantitative competition and recording medium having recorded thereon the program
Verfahren, Vorrichtung und Programm fur quantitative Wettkampfe und Aufzeichungsmedium, welches das Programm gespeichert hat
Systeme, methode et programme pour la concurrence quantitative et medium de stockage pour le programme associe
PATENT ASSIGNEE:
NIPPON TELEGRAPH AND TELEPHONE CORPORATION, (2460174), 3-1, Otemachi 2-chome, Chiyoda-ku, Tokyo 100-8116, (JP), (Proprietor designated states: all)
INVENTOR:
Chida, Koji, NTT Intellectual Property Center, 9-11, Midori-cho 3-chome, Musashino-shi, Tokyo 180-8585, (JP)
Kobayashi, Kunio, NTT Intellectual Property Center, 9-11, Midori-cho 3-chome, Musashino-shi, Tokyo 180-8585, (JP)
Morita, Hikaru, NTT Intellectual Property Center, 9-11, Midori-cho 3-chome, Musashino-shi, Tokyo 180-8585, (JP)

LEGAL REPRESENTATIVE:
  Hoffmann, Eckart (5571), Patentanwalt, Bahnhofstrasse 103, 82166 Grafelfing, (DE)
PATENT (CC, No, Kind, Date): EP 1225530 A1 020724 (Basic)
                             EP 1225530 B1 051026
APPLICATION (CC, No, Date): EP 2002001009 020117;
PRIORITY (CC, No, Date): JP 200110327 010118
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): G06F-017/60
CITED REFERENCES (EP B):
  KIKUCHI H.; HOTTA S.; ABE K.; NAKANISHI S.: 'distributed auction servers resolving winner and winning bid without revealing privacy of bids' PARALLEL AND DISTRIBUTED SYSTEMS: WORKSHOPS, SEVEN INTERNATIONAL CONFERENCE ON 04 July 2000 - 07 July 2000, LOS ALAMITOS, pages 307 - 312;

ABSTRACT EP 1225530 A1
  Numbers 1, 2, ..., M are assigned to bidding prices from the minimum to maximum values V1)) to VN)). For a bidding value Vvi)) each user 11-i generates two sequences of information si))=(si,1)), si,2, ...,)) si,M))) and ti))=(ti,1,)) ti,2,)) ..., ti,M))) such that si,1))=ti,1)), ..., si,vi-1))=ti,vi-1)), si,vi))(not equal to)ti,vi)), ..., si,M))(not equal to)ti,M)), then secretly sends the two sequences of information s; and t; to quantitative competition apparatuses 15A and 15B, respectively, and sends hash values H1i))=h(si))) and H2i))=h(ti))) of the two sequences of information si)) and ti)) and a hash value h(Vvi))(parallel to)ri))) containing an intended value Vvi)) to a bulletin board apparatus 21. The quantitative competition apparatuses 15A and 15B extract w-th elements si,w)) from respective sequences s1)) to sN)) and w-th elements ti,w)) from respective sequences t1)) to tN)), then create a concatenation Seqs,w)) of N elements si,w)) and a concatenation Seqt,w)) of N elements ti,w)), then compare them using a one-way function without revealing their values, and, if they differ, deciding that the intended value Vvi)) equal to or smaller than a value Vw)) is present, and determines the minimum value by changing w.
ABSTRACT WORD COUNT: 189
NOTE:
  Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):
 Application: 020724 A1 Published application with search report
 Examination: 020724 A1 Date of request for examination: 20020117
 Examination: 030416 A1 Date of dispatch of the first examination report: 20030226
 Grant: 051026 B1 Granted patent
 Change: 061004 B1 Title of invention (German) changed: 20061004
 Change: 061004 B1 Title of invention (English) changed: 20061004
 Change: 061004 B1 Title of invention (French) changed: 20061004
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language   Update   Word Count
      CLAIMS A (English) 200230   5122
      CLAIMS B (English) 200543   4945
      CLAIMS B   (German) 200543   4593
      CLAIMS B   (French) 200543   5249
      SPEC A   (English) 200230   9495
      SPEC B   (English) 200543   9744
Total word count - document A   14620
Total word count - document B   24531
Total word count - documents A + B   39151

...SPECIFICATION to some extent, and if the number of bits of each element is large, the random numbers R1i)) and R2i)) may be omitted .

The quantitative competition apparatuses 15A (and 15B) comprise, as shown in Fig. 4 (and Fig. 5), receiving parts 40A (40B), decrypting parts 37A (47B), storage parts 41A (41B), random generating parts 42A (42B), hash function calculating...

...SPECIFICATION to some extent, and if the number of bits of each element is large, the random numbers R1i)) and R2i)) may be omitted .
The quantitative competition apparatuses 15A (and 15B) comprise, as shown in Fig. 4 (and Fig. 5), receiving parts 40A (40B), decrypting parts 37A (47B), storage parts 41A (41B), random generating parts 42A (42B), hash function calculating...

20/5,K/16 (Item 16 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01217622
Optical disk, optical disk recording and reproducing apparatus, and method for recording and reproducing
Optische Platte, optisches Plattenaufzeichnungs- und wiedergabegerat, und Verfahren zur Aufzeichnung und Wiedergabe
Disque optique, appareil pour l'enregistrement et la reproduction de disque optique, et methode d'enregistrement et de reproduction
PATENT ASSIGNEE:
Matsushita Electric Industrial Co., Ltd., (1855508), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Proprietor designated states: all)
INVENTOR:
Nagai, Takahiro, Mezon Higashinoda-cho 301, 4-23, Higashinoda-cho, 4-chome, Miyakojima-ku, Osaka-shi, Osaka 534-0024, (JP)
Ishihara, Hideshi, 10-120, Ikuno 1-chome, Katano-shi, Osaka 576-0054, (JP)
Takagi, Yuji, 2-29-1-309, Deguchi, Hirakata-shi, Osaka 573-0065, (JP)
Yumiba, Takashi, Bervi Nishiura 606, Kowata-nishiura 58, Uji-shi, Kyoto 611-0002, (JP)
Shoji, Mamoru, 3-13-4-805, Mozu-umemachi, Sakai-shi, Osaka 591-8032, (JP)
Oshima, Mitsuaki, 115-3, Katsura-minamitatsumi-cho, Nishikyo-ku, Kyoto-shi, Kyoto 615-8074, (JP)
Ohara, Shunji, 221-5, Shinjo, Higashiosaka-shi, Osaka 578-0963, (JP)
Ito, Motoshi, 17-25-302, Furuichi 3-chome, Joto-ku, Osaka-shi, Osaka 536-0001, (JP)
Ishida, Takashi, 13-14, Hashimoto-isoku, Yawata-shi, Kyoto 614-8331, (JP)
Nakamura, Atsushi, Syoukouryo, 25-3, Mido-cho, Kadoma-shi, Osaka 571-0064 , (JP)
Tadashi, Jahana, Dai-5 Mine Haitsu 202, 836-6, Kamoi, Midori-ku, Yokohama-shi, Kanagawa 226-0003, (JP)
Nakata, Kouhei, Eminensu Marunouchi B305, 13-15, Marunouchi-cho, Kawanishi-shi, Hyogo 666-0003, (JP)
LEGAL REPRESENTATIVE:
Eisenfuhr, Speiser & Partner (100151), Patentanwalte Rechtsanwalte Postfach 10 60 78, 28060 Bremen, (DE)
PATENT (CC, No, Kind, Date): EP 1058254 A2 001206 (Basic)
EP 1058254 A3 011121
EP 1058254 B1 040707
APPLICATION (CC, No, Date): EP 2000108910 000427;
PRIORITY (CC, No, Date): JP 99122104 990428; JP 99128197 990510; JP 99299635 991021
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
RELATED DIVISIONAL NUMBER(S) - PN (AN):
(EP 2004004964)
INTERNATIONAL PATENT CLASS (V7): G11B-020/00; G11B-007/007; G11B-023/28; G06F-001/00
CITED PATENTS (EP B): EP 442566 A; EP 802527 A; EP 954173 A; EP 984346 A;

WO /21087 A; WO 98/58368 A; GB 2332977 A; US 5513169 A; US 5596639 A; US 5646993 A; US 5745568 A; US 5752009 A

CITED REFERENCES (EP B):

PATENT ABSTRACTS OF JAPAN vol. 1997, no. 10, 31 October 1997 (1997-10-31) & JP 09 171619 A (SONY CORP), 30 June 1997 (1997-06-30)

PATENT ABSTRACTS OF JAPAN vol. 2000, no. 07, 29 September 2000 (2000-09-29) & JP 2000 113586 A (VICTOR CO OF JAPAN LTD), 21 April 2000 (2000-04-21);

ABSTRACT EP 1058254 A2

An optical disk of recording type on which data is recordable is provided which includes a data recording and reproducing area (102) for recording data therein and reproducing data therefrom, and a read-only disk identification information area (104) for recording disk identification information (107) for identifying the optical disk therein. In the optical disk, the disk identification information (107) is formed by removing a reflection film formed on the optical disk in a strip shape. The disk identification information (107) includes an inherent disk identifier for each optical disk, and the data recording and reproducing area includes an area for recording therein encrypted data, which is encrypted using information including the disk identification information for identifying the optical disk as a key.

ABSTRACT WORD COUNT: 123

NOTE:

Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	001206	A2	Published application without search report
Change:	001220	A2	Title of invention (French) changed: 20001101
Search Report:	011121	A3	Separate publication of the search report
Examination:	020717	A2	Date of request for examination: 20020508
Examination:	020925	A2	Date of dispatch of the first examination report: 20020807
Change:	031022	A2	Title of invention (German) changed: 20030902
Change:	031022	A2	Title of invention (English) changed: 20030902
Change:	031022	A2	Title of invention (French) changed: 20030902
Change:	040428	A2	Application number of divisional application (Article 76) changed: 20040309
Grant:	040707	B1	Granted patent
Change:	040804	B1	Inventor information changed: 20040611
Change:	040804	B1	Inventor information changed: 20040611
Oppn None:	050629	B1	No opposition filed: 20050408

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200049	5366
CLAIMS B	(English)	200428	1383
CLAIMS B	(German)	200428	1161
CLAIMS B	(French)	200428	1704
SPEC A	(English)	200049	30838
SPEC B	(English)	200428	28902
Total word count - document A			36210
Total word count - document B			33150
Total word count - documents A + B			69360

...SPECIFICATION so as to be divided into the first decipher key area 2201 having a division decipher key of 4 bytes and the second decipher key area 2202 having a division decipher key of 4 bytes. Therefore, in spite of the size of the encrypted content recorded...

...sectors, a plurality of sectors (2 sectors in Fig. 27) are utilized. In this case, dummy data is recorded in the unused area as complementary data. In an example of Fig. 27, complementary data 2203 for one...

...SPECIFICATION so as to be divided into the first decipher key area 2201 having a division decipher key of 4 bytes and the second decipher key area 2202 having a division decipher key of 4 bytes. Therefore, in spite of the size of the encrypted content recorded...

...sectors, a plurality of sectors (2 sectors in Fig. 27) are utilized. In this case, dummy data is recorded in the unused area as complementary data. In an example of Fig. 27, complementary data 2203 for one...

20/5,K/19 (Item 19 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01150840
Image data reproducing method, image data reproducing apparatus, image data recording method and image data recording apparatus
Bilddatenwiedergabeverfahren, Bilddatenwiedergabeanlage, Bilddatenaufnahmeverfahren, und Bilddatenaufnahmeanlage
Procede de reproduction de donnees d'image, appareil de reproduction de donnees d'image, procede d'enregistrement de donnees d'image, et appareil d'enregistrement de donnees d'image
PATENT ASSIGNEE:
Pioneer Corporation, (2812420), 4-1 Meguro 1-chome, Meguro-ku, Tokyo, (JP), (Applicant designated States: all)
INVENTOR:
Inoshita, Gen, Pioneer Corporation, Ohmori Works., 15-5 Ohmorinishi 4-chome, Ohta-ku, Tokyo-to, (JP)
Sugita, Keizo, Pioneer Corporation, Ohmori Works., 15-5 Ohmorinishi 4-chome, Ohta-ku, Tokyo-to, (JP)
Funamoto, Kyota, Pioneer Corporation, Tokorozawa Works., No. 2610 Hanazono 4-chome, Tokorozawa-shi, Saitama-ken, (JP)
LEGAL REPRESENTATIVE:
Klingseisen, Franz, Dipl.-Ing. et al (6557), Patentanwalte, Dr. F. Zumstein, Dipl.-Ing. F. Klingseisen, Postfach 10 15 61, 80089 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1003338 A2 000524 (Basic)
EP 1003338 A3 020703
APPLICATION (CC, No, Date): EP 99122075 991116;
PRIORITY (CC, No, Date): JP 98326937 981117
DESIGNATED STATES: DE; FR; NL
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): H04N-009/82

ABSTRACT EP 1003338 A2
A method of reproducing first images and second images simultaneously, synchronizing them with each other. The method includes the processes of: reading first image data representing the first images and second image data representing the second images from a recording medium (1); storing the first image data into a first memory device (58) and storing the second image data into a second memory device (59); and separately and simultaneously decoding the first image data and the second image data by using a first decoding device (61) and a second decoding device (62). In this method, each of the first image data and the second image data is divided into a plurality of data units (43) each having an equal time length and an equal data size, and each of the data units (43a) of the first image data and each of the data units (43b) of the second image data are alternately arranged on the recording medium (1).
ABSTRACT WORD COUNT: 159
NOTE:
Figure number on first page: 3

LEGAL STATUS (Type, Pub Date, Kind, Text):
 Application: 000524 A2 Published application without search report
 Search Report: 020703 A3 Separate publication of the search report
 Examination: 020925 A2 Date of request for examination: 20020722
 Change: 070110 A2 Title of invention (German) changed: 20070110
 Change: 070110 A2 Title of invention (English) changed: 20070110
 Change: 070110 A2 Title of invention (French) changed: 20070110
 Change: 070801 A2 Title of invention (German) changed: 20070801
 Change: 070801 A2 Title of invention (English) changed: 20070801
 Change: 070801 A2 Title of invention (French) changed: 20070801
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200021	2065
SPEC A	(English)	200021	11293
Total word count - document A			13358
Total word count - document B			0
Total word count - documents A + B			13358

...SPECIFICATION rate, predetermined dummy data are written into this portion. At the time of reproduction, the **dummy** data are identified and are **not** used for the **decoding** process by means of MPEG2. In another way, the dummy data may be null data which are ignored at the time of the **decoding** process.
Image data are compressed and encoded so that a predetermined number of bits are...

20/5,K/21 (Item 21 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00943762
Method for the settlement of credit by an IC card
Verfahren zur Regelung von Gutschriften mittels einer Chipkarte
Methode d'etablissement de paiements par carte de credit
PATENT ASSIGNEE:
NIPPON TELEGRAPH AND TELEPHONE CORPORATION, (686339), 19-2 Nishi-Shinjuku 3-chome, Shinjuku-ku, Tokyo 163-19, (JP), (Proprietor designated states: all)
INVENTOR:
Ishiguro, Ginya, Gurin Haitsu, 12-2-403, 580, Nagasawa, Yokosuka-shi, Kanagawa, (JP)
Muta, Toshiyasu, 60-95, Sachigaoka, Asahi-ku, Yokohama-shi, Kanagawa 241-0822, (JP)
Sakita, Kazutaka, 2-14-1-613, Kaneya, Yokosuka-shi, Kanagawa, (JP)
Miyaguchi, Shoji, 1-4-4, Sugano,, Ichikawa-shi, Chiba, (JP)
Okamoto, Tatsuaki, 94-2-5-503, Nagasawa, Yokosuka-shi, Kanagawa, (JP)
Fujioka, Atsushi, B-305, 9-2-12, Sugita, Isogo-ku, Yokohama-shi, Kanagawa , (JP)
LEGAL REPRESENTATIVE:
Hoffmann, Eckart, Dipl.-Ing. (5571), Patentanwalt, Bahnhofstrasse 103, 82166 Grafelfing, (DE)
PATENT (CC, No, Kind, Date): EP 856822 A2 980805 (Basic)
EP 856822 A3 981021
EP 856822 B1 030305
APPLICATION (CC, No, Date): EP 98104504 930916;
PRIORITY (CC, No, Date): JP 92249293 920918; JP 92249294 920918; JP 92308688 921118; JP 92317254 921126; JP 92317255 921126
DESIGNATED STATES: DE; FR; GB
RELATED PARENT NUMBER(S) - PN (AN):
EP 588339 (EP 93114917)
INTERNATIONAL PATENT CLASS (V7): G07F-007/10
CITED PATENTS (EP B): EP 82958 A; EP 281059 A; EP 421409 A; EP 422230 A; EP

461983 A; EP 475837 A; WO 91/16691 A

ABSTRACT EP 856822 A2
An IC card (6) has a card information memory area wherein there are written a card identification number IDU, a predetermined setting number Ns, a first master digital signature SA4 for said setting number Ns and a second master digital signature SA5 for information including said card identification number IDU and said first master digital signature SA4. An IC card terminal (2a, 2b) has terminal information memory area wherein there are written a master public key nA for verification of a master digital signature, terminal secret keys pT and qT for the creation of a terminal digital signature and a terminal public key nT for verification of said terminal digital signature. When inserted into the IC card terminal, said IC card transmits said card identification number IDU and said first and second master digital signatures to said IC card terminal; said IC card terminal verifies said second master digital signature SA5 and, if valid, instructs the entering of a password and transmits a password Nc' to said IC card when it is entered; said IC card matches said password Nc' with a password Nc stored in said card information memory means and, if they match, transmits an authentication signal to said IC card terminal; and upon receiving said authentication signal said IC card terminal becomes enabled for providing a service and, after completion of said service, records information including an amount value V for said service and said received card identification number IDU, as usage/management information in usage/management memory means.
ABSTRACT WORD COUNT: 251
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Change:	020710	A2 Title of invention (German) changed: 20020523
Examination:	20000315	A2 Date of dispatch of the first examination report: 20000127
Oppn None:	040225	B1 No opposition filed: 20031208
Change:	020710	A2 Title of invention (French) changed: 20020523
Change:	020710	A2 Title of invention (English) changed: 20020523
Grant:	030305	B1 Granted patent
Application:	980805	A2 Published application (A1with Search Report ;A2without Search Report)
Examination:	980805	A2 Date of filing of request for examination: 980312
Change:	980909	A2 Inventor (change)
Change:	981007	A2 Inventor (change)
Search Report:	981021	A3 Separate publication of the European or International search report

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	199832	882
CLAIMS B	(English)	200310	1106
CLAIMS B	(German)	200310	1008
CLAIMS B	(French)	200310	1351
SPEC A	(English)	199832	14787
SPEC B	(English)	200310	14923
Total word count - document A			15672
Total word count - document B			18388
Total word count - documents A + B			34060

...SPECIFICATION function to simplify the processing of the IC card system.

Also it is possible to omit either one of the random number R and X although security decreases. Conversely, by prestoring algorithms for encipherment of information to be transmitted and a common key for encipherment and decipherment in memories of the IC card 6 and the IC

card terminal 2, the mutual...

...SPECIFICATION function to simplify the processing of the IC card system.

Also it is possible to omit either one of the random number R and X although security decreases. Conversely, by prestoring algorithms for encipherment of information to be transmitted and a common key for encipherment and decipherment in memories of the IC card 6 and the IC card terminal 2, the mutual...

20/5,K/27 (Item 27 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00655909
Method and apparatus for waveform shaping of packet data
Verfahren und Einrichtung zur Signalformung von Paketdaten
Procede et dispositif de mise en forme de donnees en paquets
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Proprietor designated states: all)
INVENTOR:
URABE, Yoshio, 8126-105 Takayama-cho, Ikoma-shi, Nara 630-0101, (JP)
KOGA, Shouichi, 542, Edakuni, Honami-machi, Kaho-gun, Fukuoka-ken, 820, (JP)
TAKAI, Hitoshi, 3-17-11, Higashitokiwadai, Toyono-cho, Toyono-gun, Osaka 563-01, (JP)
KAI, Koji, 2-2-46-402, Higashi-Hirao Hakata-ku, Fukuoka-shi, Fukuoka 816-0053, (JP)
YAMASAKI, Hidetoshi, 9-39-7, Higashisonoda-cho, Amagasaki-shi, Hyogo-ken 661, (JP)
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721), Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 631398 A2 941228 (Basic)
EP 631398 A3 000308
EP 631398 B1 041117
APPLICATION (CC, No, Date): EP 94109760 940623;
PRIORITY (CC, No, Date): JP 93154776 930625; JP 93223292 930908; JP 9413760 940207
DESIGNATED STATES: DE; FR; GB; NL
RELATED DIVISIONAL NUMBER(S) - PN (AN):
EP 1333633 (EP 2003008489)
EP 1331778 (EP 2003008498)
INTERNATIONAL PATENT CLASS (V7): H04L-025/03; H03G-003/30; H04L-027/20
CITED PATENTS (EP B): EP 369135 A; EP 463625 A; EP 494696 A; EP 545546 A; EP 588424 A; DE 3941265 A; US 3912863 A; US 5140613 A; US 5412691 A
CITED REFERENCES (EP B):
PATENT ABSTRACTS OF JAPAN vol. 016, no. 475 (E-1273), 2 October 1992 (1992-10-02) & JP 04 170128 A (MATSUSHITA ELECTRIC IND CO LTD), 17 June 1992 (1992-06-17)
ALLAN R D ET AL: "A HIGH PERFORMANCE SATELLITE DATA MODEM USING REAL-TIME DIGITAL SIGNAL PROCESSING TECHNIQUES" JOURNAL OF THE INSTITUTION OF ELECTRONIC AND RADIO ENGINEERS, vol. 58, no. 3, 1 May 1988 (1988-05-01), pages 117-124, XP000760573
PATENT ABSTRACTS OF JAPAN vol. 008, no. 261 (E-281), 30 November 1984 (1984-11-30) & JP 59 132267 A (NIPPON DENKI KK), 30 July 1984 (1984-07-30)
POLOZEC LE X ET AL: "A FAST AUTOMATIC GAIN CONTROL FOR A RF AMPLIFIER USED IN A DCS1800 (PCN) BASE STATION TRANSMITTER" PROCEEDINGS OF THE 23RD. EUROPEAN MICROWAVE CONFERENCE, MADRID, SEPT. 6 - 9, 1993, 6 September 1993 (1993-09-06), pages 935-938, XP000630037 EUROPEAN MICROWAVE CONFERENCE MANAGEMENT COMMITTEE ISBN: 0-946821-23-2

PATENT ABSTRACTS OF JAPAN vol. 017, no. 676 (E-1475), 13 December 1993 (1993-12-13) & JP 05 227232 A (HITACHI LTD;OTHERS: 01), 3 September 1993 (1993-09-03);

ABSTRACT EP 631398 A2

In the transmitter which carries out burst transmission using information data as a packet, if the status is divided into four modes, namely, burst stop mode, burst rising mode, burst continuous mode, and burst falling mode,

a waveform shaping equipment designed to read out shaped waveform data for each mode from outputs of either of the two memory tables, the first memory table which holds waveform data for specific data patterns used in common in burst rising mode and burst falling mode and the second memory table which holds waveform data for all data patterns used in the burst continuous mode, or a waveform shaping equipment comprising the third memory table which holds waveform data corresponding to all the data patterns used in the burst rising mode and the fourth memory table which holds waveform data corresponding to all data patterns used in the burst falling mode and generating shaped waveform data by synthesizing the two outputs of the third and the fourth memory tables at the time of burst continuous mode. (see image in original document)

ABSTRACT WORD COUNT: 179

NOTE:

Figure number on first page: 13

LEGAL STATUS (Type, Pub Date, Kind, Text):

Examination:	000802 A2	Date of request for examination: 20000607
Change:	20000223 A2	International Patent Classification changed: 20000106
Oppn None:	051109 B1	No opposition filed: 20050818
Change:	031029 A2	Inventor information changed: 20030906
Examination:	021211 A2	Date of dispatch of the first examination report: 20021028
Change:	020417 A2	International Patent Classification changed: 20020301
Change:	030604 A2	Application number of divisional application (Article 76) changed: 20030416
Grant:	041117 B1	Granted patent
Application:	941228 A2	Published application (A1with Search Report ;A2without Search Report)
Search Report:	20000308 A3	Separate publication of the search report
Change:	990915 A2	International Patent Classification changed: 19990729

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF2	7821
CLAIMS B	(English)	200447	830
CLAIMS B	(German)	200447	699
CLAIMS B	(French)	200447	1020
SPEC A	(English)	EPABF2	19850
SPEC B	(English)	200447	7855
Total word count - document A			27676
Total word count - document B			10404
Total word count - documents A + B			38080

...SPECIFICATION transmitted. In this fourth embodiment, the hardware scale with respect to the shift register, address decoder , memory, etc. increases but no complicated control means is required to change over the memory...

...the information data into the shift register in the pattern generator from the first time without using dummy data , and the time equivalent to several time slots required for transmitting dummy data strings can...

...the same principle will be applied to multilevel patterns exceeding ternary patterns, if an address decoder for converting multilevel patterns to binary address signals is provided, partial waveforms of baseband signals...

20/5,K/31 (Item 31 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00361288
Decoder circuit.
Dekodierschaltung.
Circuit decodeur.
PATENT ASSIGNEE:
FUJITSU LIMITED, (211460), 1015, Kamikodanaka Nakahara-ku, Kawasaki-shi Kanagawa 211, (JP), (applicant designated states: DE;FR;GB)
INVENTOR:
Iwazaki, Tomonobu, 6-16-4, Nishitsuruma, Yamato-shi Kanagawa 242, (JP)
LEGAL REPRESENTATIVE:
Billington, Lawrence Emlyn et al (28331), HASELTINE LAKE & CO Hazlitt House 28 Southampton Buildings Chancery Lane, London WC2A 1AT, (GB)
PATENT (CC, No, Kind, Date): EP 327340 A2 890809 (Basic)
EP 327340 A3 910320
EP 327340 B1 931006
APPLICATION (CC, No, Date): EP 89300971 890201;
PRIORITY (CC, No, Date): JP 8822285 880202
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS (V7): G11C-008/00;
CITED REFERENCES (EP A):
PATENT ABSTRACTS OF JAPAN, vol. 7, no. 78 (P-188) 1223 , 31st March 1983; & JP-A-58 6589 (HITACHI) 14-01-1983
PATENT ABSTRACTS OF JAPAN, vol. 10, no. 283 (E-440) 2339 , 26th September 1986; & JP-A-61 101 124 (HITACHI) 20-05-1986;

ABSTRACT EP 327340 A2
A decoder circuit comprises a plurality of signal conductors (X(sub 0) - X(sub 7) , DL), first potential setting units (Tpc) for setting a potential of the signal conductors (X(sub 0) - X(sub 7) , DL) to a first potential, second potential setting units (Cs) for maintaining a potential of one signal conductor (X(sub 0) - X(sub 7)) at the first potential and bringing a potential of the remaining signal conductors (X(sub 0) - X(sub 7) , DL) to a second potential, and a respective transfer transistor (T(sub 0) - T(sub 7)) provided for each signal conductor (X(sub 0) - X(sub 7)). A gate electrode of each transfer transistor (T(sub 0) - T(sub 7)) is connected to its respective signal conductor (X(sub 0) - X(sub 7)), a source electrode thereof is connected to another signal conductor (X(sub 1) - X(sub 7) , DL), and one transfer transistor (T(sub 0) - T(sub 7)) is switched ON and a decoded output signal is output when a gate potential of that transfer transistor (T(sub 0) - T(sub 7)) is maintained at the first potential and a source potential thereof is brought to the second potential. Therefore, only one output signal conductor (X(sub 0) - X(sub 7)) is selected during a decoder operation without using a discharge detecting circuit of a nonselected output signal conductor and a timing signal, and thus an operation speed of the decoder circuit is much higher and the decoding circuit has a simpler construction and is suitable as a large scale integration circuit.
ABSTRACT WORD COUNT: 258

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 890809 A2 Published application (A1with Search Report ;A2without Search Report)

Search Report: 910320 A3 Separate publication of the European or International search report
Examination: 910717 A2 Date of filing of request for examination: 910516
Examination: 930310 A2 Date of despatch of first examination report: 930126
Grant: 931006 B1 Granted patent
Oppn None: 940928 B1 No opposition filed
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPBBF1	1313
CLAIMS B	(German)	EPBBF1	964
CLAIMS B	(French)	EPBBF1	1207
SPEC B	(English)	EPBBF1	5528
Total word count - document A			0
Total word count - document B			9012
Total word count - documents A + B			9012

...SPECIFICATION level.
Figures 6 and 7 are circuit diagrams showing modifications of the embodiment of the decoder circuit shown in Fig. 5. In these decoder circuits, the dummy signal conductor DL can be omitted . As shown in Fig. 6, in one modification of the decoder circuit, output signal conductors X(sub 0) - X(sub 7) are divided into pairs of two adjacent...

...first output signal conductor X(sub 0).
As described above, in these modifications of the decoder circuit, the dummy signal conductor DL can be omitted . Furthermore, a source electrode of each of the transfer transistors T(sub 0) - T(sub 7) is...

20/5,K/36 (Item 36 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01157716 **Image available**
SYSTEM AND METHOD FOR DATA ENCRYPTION
SYSTEME ET PROCEDE DE CRYPTAGE DE DONNEES
Patent Applicant/Assignee:
XSIDES CORPORATION, 821 Second Avenue, Suite 1600, Seattle, WA 98104, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
YOUATT David P, 24539 NE 11th Street, Redmond, WA 98074, US, US (Residence), US (Nationality), (Designated only for: US)
SMITH Jason M, 15817 NE 90th, #G255, Redmond, WA 98052, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
DONOHUE Michael J (et al) (agent), 2600 Century Square, 1501 Fourth Avenue, Seattle, WA 98101-1688, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200479980 A2-A3 20040916 (WO 0479980)
Application: WO 2004US6688 20040305 (PCT/WO US04006688)
Priority Application: US 2003384147 20030305
Designated States:
(All protection types applied unless otherwise stated - for applications 2004+)
AE AG AL AM AT AU AZ BA BB BG BR BW BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE EG ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NA NI NO NZ OM PG PH PL PT RO RU SC SD SE SG SK SL SY TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW

(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) BW GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class (v7): H04N-007/167
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 12794

English Abstract
An encryption technology uses an encryption map and video graphics processing technology to combine an encryption map with the image data. Video image processing using maps, such as texture maps, bump maps and the like are combined with an encryption map to generate and encrypted image data. The image is subsequently decrypted using encryption keys that are combined with the encrypted image data using video graphics processing technologies. The decryption map is combined with the encrypted signal to generate a viewable image. The encryption keys may be on a per pixel basis with a separate encryption key for each pixel. Alternatively, an encryption key may contain active keys that may be used to decrypt more than one pixel as well as decoy keys that do not decrypt the signal and thus confound unauthorized decryption attempts. Using encryption maps, single video frames or portions of video frames may be encrypted. The encryption maps may be used with scaled image data and with two dimensional or three dimensional graphics processors.

French Abstract
L'invention porte sur une technique de cryptage utilisant une carte de cryptage et une technique de traitement de graphiques video. Le traitement des images video recourt a des cartes de texture, de reliefs, etc, combinees avec une carte de cryptage de maniere a obtenir des donnees d'image cryptees. L'image est ensuite decryptee a l'aide de clefs de cryptage qui sont combinees avec les donnees d'image cryptees a l'aide de techniques video de traitement graphique. La carte de decryptage est combinee au signal crypte pour donner une image visible. Il peut y avoir une clef de cryptage separee par pixel. En variante, une clef de cryptage peut contenir des clefs actives pouvant decrypter plus d'un pixel et des clefs leurres qui ne decryptent pas le signal et dejouent les tentatives de decryptage non autorisees. On peut a l'aide de cartes de cryptage crypter des images video uniques ou des parties d'images video. Les cartes de cryptage peuvent etre utilisees avec des donnees d'images agrandies ou reduites et avec des processeurs graphiques en 2D ou en 3D.

Legal Status (Type, Date, Text)
Publication 20040916 A2 Without international search report and to be republished upon receipt of that report.
Search Rpt 20041021 Late publication of international search report
Republication 20041021 A3 With international search report.
Republication 20041021 A3 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Search Rpt 20041021 Late publication of international search report
Claim Mod 20041223 Later publication of amended claims under Article 19 received: 20041104
Republication 20041223 A3 With international search report.
Republication 20041223 A3 With amended claims.
Fulltext Availability:
Claims

Claim

... claim 12 wherein the encrypted output image data comprises a plurality of pixels and the decryption map has a plurality of storage locations corresponding to each of the plurality of pixels in the encrypted output image data and contains active decryption data in at least one location in the decryption map, the remaining locations in the decryption map containing decoy decryption data not used to decrypt the encrypted output image data.

18 The system of claim 17 wherein the active decryption data in the at least one location is stored in a predetermined one of the plurality of locations within the decryption map.

19 The system of claim 17 wherein the active decryption data in the at least one location is stored in a pseudo-random one of...

20/5,K/38 (Item 38 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01126380 **Image available**
METHOD AND SYSTEM FOR FORWARDING A CONTROL INFORMATION
PROCEDE ET SYSTEME DE TRANSFERT D'UNE INFORMATION DE COMMANDE
Patent Applicant/Assignee:
NOKIA CORPORATION, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality)
Inventor(s):
TOSKALA Antti, Mankkaanrinne 2 C, FIN-02180 Espoo, FI,
MALKAMAKI Esa, Riippakoivuntie 17 B, FIN-02130 Espoo, FI,
Legal Representative:
UNGERER Olaf (agent), Eisenfuhr, Speiser & Partner, Arnulfstr. 25, 80335 Munich, DE,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200449749 A2-A3 20040610 (WO 0449749)
Application: WO 2003IB5361 20031112 (PCT/WO IB03005361)
Priority Application: US 2002304949 20021127
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE EG ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK
LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PG PH PL PT RO RU SC
SD SE SG SK SL SY TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) BW GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class (v7): H04Q-007/38
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 8163

English Abstract
The present invention relates to a method and system for forwarding a control information in a transmission signal of a communication network. A dummy information is provided in at least one predetermined portion of the transmission signal, and is replaced at least partly by the control information at a control device arranged on the transmission path of the transmission signal. Signaling space is thus generated by creating the

dummy information. Thereby, a fast control signaling can be provided which does not have to be originated at a network controlling functionality. Furthermore, if a dedicated link is used, less power is required and designing of new physical channel types is not required.

French Abstract
La presente invention se rapporte a un procede et un systeme de transfert d'une information de commande dans un signal de transmission d'un reseau de communication. Une information factice est acheminee dans au moins une partie predeterminee du signal de transmission et est remplacee au moins partiellement par l'information de commande au niveau d'un dispositif de commande dispose sur le trajet de transmission. Un espace de signalisation est alors genere par la creation de l'information factice. En consequence, une signalisation de commande rapide peut etre acheminee et il n'est pas necessaire qu'elle soit creee pour une fonctionnalite de commande de reseau. Par ailleurs, si la liaison utilisee est specialisee, on necessite moins de puissance et il n'est pas utile de designer de nouveaux types de canaux physiques.

Legal Status (Type, Date, Text)
Publication 20040610 A2 Without international search report and to be republished upon receipt of that report.
Search Rpt 20040902 Late publication of international search report
Republication 20040902 A3 With international search report.
Examination 20041014 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... slot.

Thus, in case of the fixed positions, portions which are most likely to be **unused** can be used as **dummy** **data** positions for forwarding the specific control signaling.

Due to the fixed positions, the bits are...

...a later interleaving function will distribute the bits. The use of flexible positions generally requires **decoding** of,the transmission format indication information. However, if the dummy information is inserted to the...
...1 0, the whole frame F has to be received before this signaling can be **decoded** .

If the signaling bits are transmitted in selected time slots, the dummy bits D are...

...e. the second interleaving in the present WCIDMA system, when the final positions are known. Non - **used** or non-replaced **dummy** **bits** D may preferably be replaced by IDTX indication bits, i.e., they are not transmitted...

20/5,K/39 (Item 39 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01028558 **Image available**
PURCHASING AID LOGISTICS APPLIANCE AND METHOD TO USE SAME
INSTRUMENT LOGISTIQUE D'AIDE A L'ACHAT ET PROCEDE D'UTILISATION ASSOCIE
Patent Applicant/Assignee:
LOCKHEED MARTIN CORPORATION, c/o Lockheed Martin Federal Systems, 1801

State Route 17C, Owego, NY 13827, US, US (Residence), US (Nationality)
Inventor(s):
CACI Joseph Claude, c/o Lockheed Martin Federal Systems, 1801 State Route 17C, Owego, NY 13827, US,
SCANLON Gregory D, c/o Lockheed Martin Federal Systems, 1801 State Route 17C, Owego, NY 13827, US,
Legal Representative:
COHEN Jerry (agent), Perkins, Smith & Cohen, LLP, One Beacon Street, Boston, MA 02108 (et al), US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200358529 A1 20030717 (WO 0358529)
Application: WO 2002US41559 20021227 (PCT/WO US0241559)
Priority Application: US 200237382 20020104
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class (v7): G06F-017/60
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 10848

English Abstract
A purchasing aid logistics appliance (10) that assists a purchaser with a shopping list generation, in-store product location, automated checkout, and financial management. The purchasing aid logistics appliance (10) is in the form of a battery (100) operated purchasing aid logistics appliance with touch screen display (50) and multimedia input/output. The purchasing aid logistics appliance (10) functions as a fiduciary aid and two-way communications device secure for managing money and processing perishable data. The purchasing aid logistics appliance (10) can function as a stand-alone device or synchronized with a user's personal computer (68) via a RF or IR link.

French Abstract
L'invention concerne un instrument logistique d'aide a l'achat (10) qui sert a un acheteur pour etablir une liste de provisions, localiser un produit en magasin, effectuer un controle de sortie automatise et realiser la gestion financiere. Cet instrument logistique d'aide a l'achat (10) se presente sous forme d'un dispositif a pile (100), dote d'un ecran tactile (50) et d'une entree/sortie multimedia. Ledit instrument logistique d'aide a l'achat (10) fonctionne comme dispositif d'aide fiduciaire et de dialogue securise pour la gestion financiere et le traitement de donnees temporaires. L'instrument logistique d'aide a l'achat (10) selon l'invention peut fonctionner en tant que dispositif autonome ou synchronise avec l'ordinateur personnel (68) d'un utilisateur par l'intermediaire d'une liaison RF ou IR.

Legal Status (Type, Date, Text)
Publication 20030717 A1 With international search report.

Patent and Priority Information (Country, Number, Date):
Patent: ... 20030717

Fulltext Availability:
  Detailed Description
Publication Year: 2003

Detailed Description
... signals 50 but is instead computed as select lines for
  B010 (BOOI+F) by address decoder 55. The central processor 11
  thinks it is writing BOOO through B003 four successive locations the
  address
  decoder 55 now gets a signal not to use the random number
  encode
  key 52 generated by random number generation circuitry 51. Now
  the central processor 11...

...commands by memory bus address signals 50
  beginning with location BOOO through B003. The address decoder
  55 functions normally but the data retrieved from these four
  locations BOOO-BOO3 is not...

 20/5,K/50   (Item 50 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00753871   **Image available**
OPTICAL DISK, OPTICAL DISK RECORDING AND REPRODUCING APPARATUS, METHOD FOR RECORDING, REPRODUCING AND DELETING DATA ON OPTICAL DISK, AND INFORMATION PROCESSING SYSTEM
DISQUE OPTIQUE, APPAREIL D'ENREGISTREMENT ET DE REPRODUCTION SUR DISQUE OPTIQUE, PROCEDE D'ENREGISTREMENT, REPRODUCTION ET EFFACEMENT DE DONNEES SUR DISQUE OPTIQUE, ET SYSTEME DE TRAITEMENT D'INFORMATIONS
Patent Applicant/Assignee:
  MATSUSHITA ELECTRIC INDUSTRIAL CO LTD, 1006, Oaza Kadoma, Kadoma-shi, Osaka 571-8501, JP, JP (Residence), JP (Nationality)
Inventor(s):
  NAGAI Takahiro, 301, Mezon Higashinoda-cho 4-23, Higashinoda-cho 4-chome, Miyakojima-ku, Osaka-shi, Osaka 534-0024, JP,
  ISHIHARA Hideshi, 10-120, Ikuno 1-chome, Katano-shi, Osaka 576-0054, JP,
  TAKAGI Yuji, 2-29-1-309, Deguchi, Hirakata-shi, Osaka 573-0065, JP,
  YUMIBA Takashi, 606, Bervi Nishiura, 58, Kowata-nishiura, Uji-shi, Kyoto 611-0002, JP,
  SHOJI Mamoru, 3-13-4-805, Mozu-umemachi, Sakai-shi, Osaka 591-8032, JP,
  OSHIMA Mitsuaki, 115-3, Katsura-minamitatsumi-cho, Nishikyo-ku, Kyoto-shi, Kyoto 615-8074, JP,
  OHARA Shunji, 221-5, Shinjo, Higashiosaka-shi, Osaka 578-0963, JP,
  ITO Motoshi, 17-25-302, Furuichi 3-chome, Joto-ku, Osaka-shi, Osaka 536-0001, JP,
  ISHIDA Takashi, 13-14, Hashimoto-isoku, Yawata-shi, Kyoto 614-8331, JP,
  NAKAMURA Atsushi, Syoukouryo, 25-3, Mido-cho, Kadoma-shi, Osaka 571-0064, JP,
  JAHANA Tadashi, 202, Dai-5 Mine Haitsu, 836-6, Kamoi, Midori-ku, Yokohama-shi, Kanagawa 226-0003, JP,
  NAKATA Kouhei, B305, Eminensu Marunouchi, 13-15, Marunouchi-cho, Kawanishi-shi, Hyogo 666-0003, JP,
Legal Representative:
  AOYAMA Tamotsu (et al) (agent), Aoyama & Partners, IMP Building, 3-7, Shiromi 1-chome, Chuo-ku, Osaka-shi, Osaka 540-0001, JP,
Patent and Priority Information (Country, Number, Date):
  Patent: WO 200067257 A2-A3 20001109 (WO 0067257)
  Application: WO 2000JP2750 20000427 (PCT/WO JP0002750)
  Priority Application: JP 99122104 19990428; JP 99128197 19990510; JP 99299635 19991021
Designated States:
(Protection type is "patent" unless otherwise stated - for applications

prior to 2004)
  CN KR
Main International Patent Class (v7): G11B-020/00
International Patent Class (v7): G11B-007/007; G11B-023/28; G06F-001/00
Publication Language: English
Filing Language: English
Fulltext Availability:
  Detailed Description
  Claims
Fulltext Word Count: 40940

English Abstract
  An optical disk of recording type on which data is recordable is provided which includes a data recording and reproducing area (102) for recording data therein and reproducing data therefrom, and a read-only disk identification information area (104) for recording disk identification information (107) for identifying the optical disk therein. In the optical disk, the disk identification information (107) is formed by removing a reflection film formed on the optical disk in a strip shape. The disk identification information (107) includes an inherent disk identifier for each optical disk, and the data recording and reproducing area includes an area for recording therein encrypted data, which is encrypted using information including the disk identification information for identifying the optical disk as a key.
French Abstract
  La presente invention concerne un disque optique de type a enregistrement sur lequel on peut enregistrer des donnees. Ce disque optique comprend une zone d'enregistrement et de reproduction de donnees concue pour y enregistrer des donnees et reproduire des donnees a partir de celle-ci, et une zone d'informations d'identification de disque ROM concue pour enregistrer les informations d'identification de disque permettant d'identifier le disque optique en question. Dans le disque optique, on constitue les informations d'identification de disque en retirant un film reflechissant applique sur le disque optique sous forme de bande. Les informations d'identification de disque comprennent un identificateur de disque inherent pour chaque disque optique, la zone d'enregistrement et de reproduction de donnees comprenant une zone d'enregistrement des donnees chiffrees, ces donnees ayant ete chiffrees en utilisant ces informations, y compris les informations d'identification de disque permettant d'identifier le disque optique comme une cle.

Legal Status (Type, Date, Text)
Publication   20001109 A2 Without international search report and to be republished upon receipt of that report.
Examination   20001228 Request for preliminary examination prior to end of 19th month from priority date
Search Rpt   20010426 Late publication of international search report
Republication 20010426 A3 With international search report.

Patent and Priority Information (Country, Number, Date):
  Patent: ... 20001109
Fulltext Availability:
  Detailed Description
Publication Year: 2000

Detailed Description
... so
  as to be divided into the first decipher key area 2201 having a division decipher key of 4 bytes and the second decipher key area 2202 having a division decipher key of 4 bytes. Therefore, in spite of the size of the encrypted content recorded...

...sectors, a plurality of sectors (2 sectors in Fig. 27) are utilized. In this case, dummy data is recorded in the unused

area as complementary data. In an example of Fig. 27t complementary data 2203 for one...

20/5,K/51 (Item 51 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00749017 **Image available**
METHODS AND APPLIANCES FOR ENCRYPTION SYSTEM VARYING DYNAMICALLY DEPENDING UPON VARIABLES AND ITS APPLICATIONS
PROCEDES ET DISPOSITIFS POUR SYSTEME DE CHIFFREMENT A VARIATION DYNAMIQUE DEPENDANT DE VARIABLES ET LEURS APPLICATIONS
Patent Applicant/Inventor:
YU Choonyeol, 712-1201 Uruk Apt., Goongrae-dong, Goonpo-si, Gyeonggi-Do 435-047, KR, KR (Residence), KR (Nationality)
Patent and Priority Information (Country, Number, Date):
Patent: WO 200062458 A2 20001019 (WO 0062458)
Application: WO 2000KR363 20000414 (PCT/WO KR0000363)
Priority Application: KR 9913182 19990414
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class (v7): H04L
Publication Language: English
Filing Language: Korean
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 4516

English Abstract
The frequencies of commercial transactions or the kind of activities on a network system have been increased gradually such as transaction with credit cards, connecting onto a banking computer system, usage of vending machines, etc. For this purpose, this invention is a password algorithm system utilizing regularly varying elements such as hour, date, week day, month, etc. that change continuously and other kinds of elements so that the password changes according to the variable elements of time and other elements. In addition, by implementing dynamic variable elements being linked to user's ID, this invention disables the abuse of private information caught by someone on the Internet as ID. Someone who gets the data as ID but not its algorithm couldn't use it as it's not accepted in a server computer system.

French Abstract
La frequence des transactions commerciales ou activites analogues sur des systemes en reseau est en progression constante, telles que les transactions avec cartes de credit, connexions a des systemes informatiques bancaires, utilisation de distributeurs automatiques, etc. A cet effet, l'invention concerne un systeme d'algorithme de mot de passe utilisant regulierement des elements variables tels que l'heure, la date, le jour de la semaine, le mois, etc. qui changent continuellement, ainsi que d'autres types d'elements, de sorte que le mot de passe change en fonction des elements variables de temps et des autres elements. De plus, par la mise en application d'elements variables dynamiques lies a

l'identite de l'utilisateur, l'invention permet d'eliminer l'utilisation abusive d'informations privees, telle l'identite, pouvant etre interceptees par une personne sur Internet. Une personne qui intercepterait les donnees d'identite mais pas leur algorithme ne pourraient pas les utiliser, car le systeme d'ordinateur de serveur ne les accepte pas.

Legal Status (Type, Date, Text)
Publication 20001019 A2 In English translation (filed in Korean).
Publication 20001019 A2 Without international search report and to be republished upon receipt of that report.
Examination 20010111 Request for preliminary examination prior to end of 19th month from priority date

Patent and Priority Information (Country, Number, Date):
Patent: ... 20001019
Fulltext Availability:
Detailed Description
Publication Year: 2000

Detailed Description
... the fingerprints and compare it to the fingerprint data that is saved. This variable coding/ decoding system has such features.

[Clause 6 1
As for clause 1, password-complicating unit is included additionally with the other password elements mentioned to intensify security. This variable coding/ decoding system has such features.

[Clause 7 1
As for clause 6, the password-complicating unit includes a dummy digit that
is not used by the computer when decoding . This variable coding/ decoding
system has such features.

[Clause 8 1
It is made up of an input unit...

...be combined using arithmetical logic units. This is the characteristic of the system for coding/ decoding of the data.

[Clause 15
As for clause 12, password-complicating unit is included additionally...

...password elements mentioned to intensify security. This is the characteristic of the system for coding/ decoding of the data.

[Clause 16 1
As for clause 15, the password-complicating unit includes a dummy digit
that is not used by the computer when decoding . This is the characteristic of the system for coding/ decoding of the data.
[Clause 17 1
A variable password lock device constituted of CPU, data...

...intensify security.

[Clause 23 1
As for clause 22, the password-complicating unit includes a dummy digit
that is not used by the computer when decoding .

[Clause 24 1

A data coding/ decoding device that is made up of CPU and a data coding/ decoding uni t, codes/ decodes data based upon variable elements
that are created naturally or artificially.

Clause 25 1
As for clause 24, the data coding/ decoding unit is saved in a data-storing device and is included additionally in the data...

...intensify security.
[Clause 28 1
As for clause 27, the password-complicating unit includes a dummy digit
that is not used by the computer when decoding .

[Clause 29 1
A fingerprint recognizing system designed

20/5,K/61 (Item 61 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00120560 **Image available**
COMPATIBLE DESCRAMBLER FOR TELEVISION SYNCHRONIZATION
DEBROUILLEUR COMPATIBLE POUR SYNCHRONISATION DE TELEVISION
Patent Applicant/Assignee:
DeRIDDER Dennis W,
MILLER Donald J,
Inventor(s):
DeRIDDER Dennis W,
MILLER Donald J,
Patent and Priority Information (Country, Number, Date):
Patent: WO 8403811 A1 19840927
Application: WO 84US402 19840316 (PCT/WO US8400402)
Priority Application: US 83961 19830316
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
GB JP
Main International Patent Class (v7): H04N-007/16
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 10119

English Abstract
A descrambling circuit for video signals which have been rendered secure against unauthorized use by suppression or elimination of the horizontal sync signals generates (29) a decoding signal at the receiving end by detection (18, 20) of an unmodified portion of the video signal occurring during the vertical blanking interval or by detection (40) of the 3.58 MHz color burst signal. In this way, descrambling can be accomplished without need for reference to a decoding signal with the scrambled video or a key inserted in the video signal at the transmission end. This also permits a single descrambling circuit to decode video signals which have been scrambled by different techniques.

French Abstract
Un circuit de debrouillage pour signaux video qui ont ete premunis contre toute utilisation non autorisee par la suppression ou l'elimination des signaux de synchronisation horizontale emet (29) un signal de decodage a l'extremite receptrice lors de la detection (18, 20)

d'une partie non modifiee du signal video se presentant pendant l'intervalle de suppression verticale ou lors de la detection (40) du signal de synchronisation de couleurs de 3,58 MHz. De cette maniere, il est possible d'effectuer un debrouillage sans avoir besoin de se referer a un signal de decodage lors d'un brouillage video ou de l'insertion d'une clef dans le signal video a l'extremite de transmission. Cela permet egalement a un seul circuit de debrouillage de decoder des signaux video qui ont ete brouilles par des procedes differents.

Patent and Priority Information (Country, Number, Date):
Patent: ... 19840927
Fulltext Availability:
Claims
Publication Year: 1984

Claim
... of the horizontal sync pulses is prevented; and
transmitting said scrambled video signal-and a- false decoding signal which cannot be used to accurately descramble the scrambled video signal.

53 A method according to claim 52, further comprising the-steps...
...unmodified signal portion of said scrambled video signal not forming a part of said false decoding signal;
generating a decoding signal solely on the basis of said detected unmodified signal portion; and
combining said scrambled...
?

File 347:JAPIO Dec 1976-2007/Jun(Updated 070926)
(c) 2007 JPO & JAPIO
File 350:Derwent WPIX 1963-2007/UD=200764
(c) 2007 The Thomson Corporation

Set	Items	Description
S1	343327	FALSE OR INVALID OR NULL OR PSUEDO OR PSEUDO OR RANDOM OR RAND OR CHAFF OR SEMIRANDOM OR PSUEDORAND? OR PSEUDORAND? OR DUMMY OR NONCE? ? OR DECOY?
S2	2540	SHILL?? OR SPOOF?? OR PHONEY? ? OR PHONY? ? OR PHONIE? ? OR FAKE? ? OR SHAM OR SHAMS
S3	30597	S1:S2(1W)(VALUE OR VALUES OR NUMBER? ? OR NUMERAL? ? OR NUMERIC?? OR ALPHANUMERIC? OR QUANTITY? ? OR QUANTITIES OR CHARACTER? ? OR BIT OR BITS OR DATA OR DATUM? ?)
S4	25500	S1:S2(1W)(DIGIT? ? OR SIGNAL? ? OR PULSE OR PULSES OR INTEGER? ? OR STRING OR STRINGS OR SUBSTRING? ? OR SEQUENCE OR SEQUENCES OR SUBSEQUENCE? ? OR NOISE OR VARIABLE? ?)
S5	13080923	USED OR USE OR USING OR USAGE? ? OR EMPLOY? OR UTILIS??? OR UTILISATION? ? OR UTILIZ??? OR UTILIZATION? ?
S6	492	NONEMPLOY? OR UNEMPLOY? OR NONUTILIS? OR NONUTILIZ? OR UNUTILIS? OR UNUTILIZ?
S7	25372	NONUSE? OR NONUSING OR NONUSAGE? OR UNUSE? OR UNUSING OR UNUSAGE? OR DISUSE? ? OR DISUSING OR DISUSAGE?
S8	330160	('NOT' OR WITHOUT OR NEVER OR CANNOT OR T) (1W)S5
S9	44477	(NON OR UN OR DIS)()S5
S10	133	S3:S4(5N)(OMIT? OR OMISSION? ? OR EXCLUD? OR EXCLUSION?)
S11	193	S3:S4(5N)S8:S9
S12	220709	DECRYPT? OR UNCRYPT? OR UNENCRYPT? OR DECOD??? OR UNENCOD?-?? OR UNCOD??? OR UNENCRYPT? OR UNENCIPHER? OR UNENCYPHER? OR DECIPHER? OR DECYPHER?
S13	39938	UNSCRAMBL? OR DESCRAMBL? OR UNCIPHER? OR UNCYPHER? OR DECOMPRESS? OR DEPACK? OR UNPACK? OR UNCOMPRESS? OR DECOMPACT? OR UNCOMPACT?
S14	28	S3:S4(5N)S6:S7
S15	49	(S10:S11 OR S14) AND S12:S13
S16	34	S15 AND PY=1963:2003
S17	20	S15 AND AY=1963:2003 AND AC=US
S18	37	S16:S17

? t18/9/2,4,10-12

18/9/2 (Item 2 from file: 347)
DIALOG(R)File 347:JAPIO

06204393 **Image available**
DIGITAL PRIVACY TELEPHONE SET

PUB. NO.: 11-145950 [JP 11145950 A]
PUBLISHED: May 28, 1999 (19990528)
INVENTOR(s): KODAMA HIROHISA
APPLICANT(s): NEC CORP
APPL. NO.: 09-312463 [JP 97312463]
FILED: November 13, 1997 (19971113)
INTL CLASS: H04L-009/20; H04L-009/12; H04L-009/36

ABSTRACT

PROBLEM TO BE SOLVED: To provide a digital privacy telephone set which can reduce speaking faults caused by the omission or erroneous insertion of data until transmission data from a caller are received on the side of a callee during privacy communication.

SOLUTION: On the side of the caller, phase information is added to

enciphered data, on the side of the callee, the phase information is detected and by comparing plural pieces of continuously or intermittently received phase information, the presence/absence of the omission or erroneous insertion of received data is detected and corrected. Besides, restored audio data outputted from a **deciphering** part 33 are received as input signals, and a data converting part 39 is provided for converting a data correspondent part and a phase information correspondent part, for which the omission is detected by data phase correcting means 37 and 38, to soundless data and outputting them. Thus, **dummy** data are inserted to the **omission** detected enciphered data part and after **descramble** processing is performed to that dummy data part and the phase information part, they are converted to the soundless data by the data converting means.

18/9/4 (Item 4 from file: 347)

05730306 **Image available**
DIGITAL SECRECY DEVICE

PUB. NO.: 10-013406 [JP 10013406 A]
PUBLISHED: January 16, 1998 (19980116)
INVENTOR(s): KODAMA HIROHISA
APPLICANT(s): NEC CORP [000423] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-163962 [JP 96163962]
FILED: June 25, 1996 (19960625)
INTL CLASS: [6] H04L-009/36; H04L-009/20; H04M-001/68
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.2 (COMMUNICATION -- Transmission Systems); 44.4 (COMMUNICATION -- Telephone)

ABSTRACT

PROBLEM TO BE SOLVED: To hold the synchronism of pseudo ransom numbers in a scramble means and a **descramble** part by adding phase information to scramble data in a transmitter-side, detecting phase information on a receiver-side and comparing a plurality of pieces of phase information which are continuously received.
SOLUTION: Phase information C generated in a data phase control part 26 is added to scramble data B from the scramble part 22 and it is transmitted to a transmission data control part 15. On the receiver-side, the presence or absence of the omission and the erroneous insertion of scramble data E is detected in a data phase detection part 37, based on phase information separated in a received data control part 36. A data phase correction part 38 estimates data quantity which is omitted end erroneously inserted by a phase correction signal from the data phase detection part 37, inserts **dummy** **data** in the **omitted** period of scramble data E and eliminates the data part of erroneously inserted scramble data E. A data conversion part 39 converts dummy data into silence data.

18/9/10 (Item 10 from file: 347)

02916268 **Image available**
DIGITAL SIGNAL REPRODUCING DEVICE

PUB. NO.: 01-213868 [JP 1213868 A]
PUBLISHED: August 28, 1989 (19890828)
INVENTOR(s): ARANO YUKARI

ONISHI TAKESHI
MATSUTANI KIYOSHI
APPLICANT(s): MITSUBISHI ELECTRIC CORP [000601] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 63-039913 [JP 8839913]
FILED: February 22, 1988 (19880222)
INTL CLASS: [4] G11B-020/10
JAPIO CLASS: 42.5 (ELECTRONICS -- Equipment)
JAPIO KEYWORD: R101 (APPLIED ELECTRONICS -- Video Tape Recorders, VTR)
JOURNAL: Section: P, Section No. 964, Vol. 13, No. 524, Pg. 119, November 22, 1989 (19891122)

ABSTRACT

PURPOSE: To ensure the reproducing of PCM data by providing a jump timing pulse generating circuit in a digital signal processing circuit and jumping a corresponding number of addresses to dummy data on the side of the readout of a memory.

CONSTITUTION: The PCM data read out of a track are demodulated by a demodulation circuit 2, and after detecting a symbol value of its header part 4 by a header detecting circuit 3, clocks corresponding to the max. sample number per field are written into a memory 5, whereas data is read out of the memory by a clock relative to a sampling frequency of a sound signal, etc., and outputted to a D/A converter 12 or an interface circuit 13. In this case, addresses of the memory 5 are generated by a DEM side address generating circuit 9, a decoding address generating circuit 8 and a D/A side address generating circuit 7 and selected by a selector 6, and then such addresses on the read side as corresponding to dummy data are jumped over by a pulse generated from the jump timing pulse generating circuit 10, thus omitting the dummy data out of the reproducing PCM data.

18/9/11 (Item 11 from file: 347)

02793026 **Image available**
WIDE RANGE MOBILE COMMUNICATION SYSTEM

PUB. NO.: 01-090626 [JP 1090626 A]
PUBLISHED: April 07, 1989 (19890407)
INVENTOR(s): MORIYAMA KAZU
APPLICANT(s): KOKUSAI ELECTRIC CO LTD [000112] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 62-245818 [JP 87245818]
FILED: October 01, 1987 (19871001)
INTL CLASS: [4] H04B-007/26
JAPIO CLASS: 44.2 (COMMUNICATION -- Transmission Systems)
JOURNAL: Section: E, Section No. 791, Vol. 13, No. 323, Pg. 156, July 21, 1989 (19890721)

ABSTRACT

PURPOSE: To attain wide range communication forming a radio communication system even with mixture of digital/analog communication systems by using a cryptographic device to a transmitter-receiver of a radio station so as to realize digital squelch.

CONSTITUTION: The cryptographic device 5 is provided with selection means No.1 and No.2, the means No.1 selects any of radio lines and a most suitable MODEM 53 thereto in each digital station, and the means No.2 switches control modes A-C of a reception signal output. The mode A is the mode operated when all the stations have the device 5 and only when a random number synchronizing signal is detected in the digital reception output of the MODEM 53 in succession to the preamble signal, a decoded

voice is outputted to a speaker 2 as a digital squelch function. The mode B is the mixed communication mode and from which of the digital and analog stations the signal is received is decided depending on the presence of the preamble signal of the receptionsection and the random number synchronizing signal, and both the stations are made receivable. The mode C is the mode receiving a signal sent from the MODEM 53 without using a random number device 52 and the digital transmission is provided to the line.

18/9/12 (Item 12 from file: 347)
DIALOG(R)File 347:JAPIO

02743947 **Image available**
COMPRESSED VOICE DATA EXCHANGE SYSTEM

PUB. NO.: 01-041547 [JP 1041547 A]
PUBLISHED: February 13, 1989 (19890213)
INVENTOR(s): IMAIZUMI YOICHI
APPLICANT(s): FUJITSU LTD [000522] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 62-198384 [JP 87198384]
FILED: August 07, 1987 (19870807)
INTL CLASS: [4] H04M-003/00
JAPIO CLASS: 44.4 (COMMUNICATION -- Telephone)
JOURNAL: Section: E, Section No. 766, Vol. 13, No. 235, Pg. 142, May 30, 1989 (19890530)

ABSTRACT

PURPOSE: To eliminate need for dividing a digital interface signal line into the talking of its own station and the relay exchange portion by adopting the constitution such that a CODEC and a format conversion section are switched depending whether or not a path is for its own station talking portion or a relay exchange portion so as to eliminate need for an analog interface line.

CONSTITUTION: A path discrimination section 4 is provided to a digital relay exchange 1 and the path deciding section 4 decides whether or not the path is for its own station talking portion or a relay exchange portion and a changeover means 7 of a multiplexer 2 is turned to the position show in solid lines in case of the own station talking, the signal is through a digital interface signal line 3 and a CODEC 5 to compress the signal at the sender side into a signal rate of 16Kbps or below and to unpack the signal at the receiver side into a rate of 64Kbps for the talking purpose. In case of relay exchange, the changeover means 7 is turned to the position shown in dotted lines, the signal is through a format conversion section 6 at the reception side to bring the signal of 16Kbps or below into a signal of 64Kbps through the addition of a dummy signal, the result is sent to the exchange 1 via the digital interface signal line 3 and exchanged and then sent to the format exchange section 6 of the multiplexer 2 via the digital interface signal line 3, where the dummy signal is excluded and the signal is restored to the original 16Kbps signal and the result is sent to an opposite station.
? t18/69,k/20,32

18/69,K/20 (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0012963821 - Drawing available
WPI ACC NO: 2003-040953/ 200303
XRPX Acc No: N2003-032065
Generating digital bitstream for data rate compression by processing input data blocks to produce shorter blocks with adaptive bit allocation

Patent Assignee: DOLBY LAB LICENSING CORP (DOLB)
Inventor: TRUMAN M M; WATSON M A
Patent Family (3 patents, 98 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
WO 2002091361	A1	20021114	WO 2002US3705	A	20020208	200303	B
AU 2002235537	A1	20021118	AU 2002235537	A	20020208	200452	E
US 6807528	B1	20041019	US 2001851589	A	20010508	200469	E

Priority Applications (no., kind, date): US 2001851589 A 20010508

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
WO 2002091361	A1	EN	15	2	

National Designated States,Original: AE AG AL AM AT AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
Regional Designated States,Original: AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW
AU 2002235537 A1 EN Based on OPI patent WO 2002091361

Alerting Abstract WO A1
NOVELTY - Method consists in capturing blocks of input data and processing them to produce shorter blocks in which some bits allocated from a pool by an adaptive allocation process represent input data, some, which are those remaining in the pool do not and can represent other information, and assembling the shorter blocks to deliver the digital bitstream.
DESCRIPTION - There is an INDEPENDENT CLAIM for a method of processing a digital bitstream.
USE - Method is for low bit rate audio encoding and decoding systems such as **Dolby Digital** and MPEG-2 AAC.
ADVANTAGE - Method uses wasted bits to carry information, so that there is no need to decode and re -encode the bitstream.
DESCRIPTION OF DRAWINGS - The figure shows a **Dolby Digital** encoder.

Title Terms/Index Terms/Additional Words: GENERATE; DIGITAL; BITSTREAM; DATA; RATE; COMPRESS; PROCESS; INPUT; BLOCK; PRODUCE; SHORT; ADAPT; BIT; ALLOCATE

Class Codes
International Classification (Main): G10L-019/00, G10L-021/04
(Additional/Secondary): H04B-001/66
US Classification, Issued: 704229000, 704500000, 370528000

File Segment: EngPI; EPI;
DWPI Class: W04; P86
Manual Codes (EPI/S-X): W04-V10G1J

Alerting Abstract ...USE - Method is for low bit rate audio encoding and decoding systems such as Dolby Digital and MPEG-2 AAC...

...ADVANTAGE - Method uses wasted bits to carry information, so that there is no need to decode and re -encode the bitstream...

Original Publication Data by Authority

Original Abstracts:
...audio encoding systems, including Dolby Digital and MPEG-2 AAC generate data streams in which unused dummy, fill, stuffing, or null bits exist whenever the bit allocation function in the encoder does not utilize all available bits from a bit pool...

...encoding, a modified encoder may insert information-carrying bits in some or all of the unused bit positions instead of null bits during the encoding process.

...
...

18/69,K/32 (Item 18 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0007174277 - Drawing available
WPI ACC NO: 1995-214940/ 199528
Related WPI Acc No: 1994-048342
XRPX Acc No: N1995-168565
EMI suppression coding - psuedorandomises positive and negative going transitions used to represent one binary state in transmitted digital signal
Patent Assignee: TUT SYSTEMS INC (TUTS-N)
Inventor: GRAHAM M H
Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
US 5422919	A	19950606	US 1992964508	A	19921021	199528 B
			US 1993150451	A	19931110	

Priority Applications (no., kind, date): US 1992964508 A 19921021; US 1993150451 A 19931110

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 5422919	A	EN	6	5	Continuation of application US 1992964508
					Continuation of patent US 5283807

Alerting Abstract US A
The method for communicating binary data uses one binary data state represented by either one of two different signal levels. Another binary data state is represented by another signal level different from the two different signal levels. A pseudorandom signal is generated. One of the two different signal levels is selected as a function of the pseudorandom signal . The binary data is recovered without the use of the pseudorandom signal .
Pref., the pseudorandom signal has a stream of pseudorandom digital signals. A third signal level may be selected to identify the other binary state.
USE/ADVANTAGE - Encoding mechanism using three distinct signal characteristics. Does not require descrambling .

Title Terms/Index Terms/Additional Words: EMI; SUPPRESS; CODE; POSITIVE; NEGATIVE; TRANSITION; REPRESENT; ONE; BINARY; STATE; TRANSMIT; DIGITAL; SIGNAL

Class Codes
International Classification (Main): H04L-027/30
US Classification, Issued: 375200000, 380034000, 380046000, 380049000

File Segment: EPI;
DWPI Class: W02
Manual Codes (EPI/S-X): W02-K05A1; W02-K05B1; W02-K05B5

Alerting Abstract ...generated. One of the two different signal levels is

selected as a function of the pseudorandom signal . The binary data is recovered without the use of the pseudorandom signal .
...

...USE/ADVANTAGE - Encoding mechanism using three distinct signal characteristics. Does not require descrambling .

Original Publication Data by Authority

Original Abstracts:
...format. By pseudorandomizing the selection of these transitions, substantial spreading of the spectral energy occurs. Descrambling need not occur since each transition is recognized as the encoded binary state. Thus, the data sender can encode...
Claims:
...for selecting between said two different signal levels under control of said pseudorandom signal; a decoder comprising means for recognizing said two different signal levels as representing said one binary state without the use of said pseudorandom signal ; and , a link coupled between said encoder and decoder.
?

```
File   2:INSPEC 1898-2007/Sep W5
         (c) 2007 Institution of Electrical Engineers
File   6:NTIS 1964-2007/Oct W2
         (c) 2007 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1884-2007/Sep W5
         (c) 2007 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2007/Oct W1
         (c) 2007 The Thomson Corp
File  35:Dissertation Abs Online 1861-2007/Jul
         (c) 2007 ProQuest Info&Learning
File  65:Inside Conferences 1993-2007/Oct 10
         (c) 2007 BLDSC all rts. reserv.
File  95:TEME-Technology & Management 1989-2007/Sep W5
         (c) 2007 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2007/Sep
         (c) 2007 The HW Wilson Co.
File 144:Pascal 1973-2007/Sep W4
         (c) 2007 INIST/CNRS
File 256:TecInfoSource 82-2007/Jul
         (c) 2007 Info.Sources Inc
File 266:FEDRIP 2007/Sep
         Comp & dist by NTIS, Intl Copyright All Rights Res
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 2006 The Thomson Corp
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
File  56:Computer and Information Systems Abstracts 1966-2007/Sep
         (c) 2007 CSA.
File  60:ANTE: Abstracts in New Tech & Engineer 1966-2007/Aug
         (c) 2007 CSA.

Set     Items   Description
S1    1434308   FALSE OR INVALID OR NULL OR PSUEDO OR PSEUDO OR RANDOM OR -
              RAND OR CHAFF OR SEMIRANDOM OR PSUEDORAND? OR PSEUDORAND? OR -
              DUMMY OR NONCE? ? OR DECOY?
S2      60321   SHILL??  OR SPOOF?? OR PHONEY? ? OR PHONY? ? OR PHONIE? ? -
              OR FAKE? ? OR SHAM OR SHAMS
S3      37005   S1:S2(1W)(VALUE OR VALUES OR NUMBER? ? OR NUMERAL? ? OR NU-
              MERIC?? OR ALPHANUMERIC? OR QUANTITY? ? OR QUANTITIES OR CHAR-
              ACTER? ? OR BIT OR BITS OR DATA OR DATUM? ?)
S4     122794   S1:S2(1W)(DIGIT? ? OR SIGNAL? ? OR PULSE OR PULSES OR INTE-
              GER? ? OR STRING OR STRINGS OR SUBSTRING? ? OR SEQUENCE OR SE-
              QUENCES OR SUBSEQUENCE? ? OR NOISE OR VARIABLE? ?)
S5   23306046   USED OR USE OR USING OR USAGE? ? OR EMPLOY? OR UTILIS??? OR
               UTILISATION? ? OR UTILIZ??? OR UTILIZATION? ?
S6      39140   NONEMPLOY? OR UNEMPLOY? OR NONUTILIS? OR NONUTILIZ? OR UNU-
              TILIS? OR UNUTILIZ?
S7      20094   NONUSE? OR NONUSING OR NONUSAGE? OR UNUSE? OR UNUSING OR U-
              NUSAGE? OR DISUSE? ? OR DISUSING OR DISUSAGE?
S8     227500   ('NOT' OR WITHOUT OR NEVER OR CANNOT OR T) (1W)S5
S9       4735   (NON OR UN OR DIS)()S5
S10       109   S3:S4(5N)(OMIT? OR OMISSION? ? OR EXCLUD? OR EXCLUSION?)
S11        90   S3:S4(5N)S8:S9
S12    161550   DECRYPT? OR UNCRYPT? OR UNENCRYPT? OR DECOD??? OR UNENCOD?-
              ?? OR UNCOD??? OR UNENCRYPT? OR UNENCIPHER? OR UNENCYPHER? OR
              DECIPHER? OR DECYPHER?
S13     52854   UNSCRAMBL? OR DESCRAMBL? OR UNCIPHER? OR UNCYPHER? OR DECO-
              MPRESS? OR DEPACK? OR UNPACK? OR UNCOMPRESS? OR DECOMPACT? OR
              UNCOMPACT?
S14        11   S3:S4(5N)S6:S7
S15         1   (S10:S11 OR S14) AND S12:S13
S16      1654   AU=(CHEUNG T? OR CHEUNG, T?)
S17         5   S16 AND S3:S4
```

S18 5 S17 NOT S15
S19 2 RD (unique items)

? t15/7

15/7/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

04777008 INSPEC Abstract Number: C91000799
Title: Inversion in time (connectionist systems)
Author(s): Thrun, S.; Linden, A.
Author Affiliation: Gesellschaft fur Math. und Datenverarbeitung mbH, Augustin, West Germany
Conference Title: Neural Networks. EURASIP Workshop 1990 Proceedings p.130-40
Editor(s): Almeida, L.B.; Wellekens, C.J.
Publisher: Springer-Verlag, Berlin, West Germany
Publication Date: 1990 Country of Publication: West Germany ix+276 pp.
ISBN: 3 540 52255 7
Conference Sponsor: Eur. Assoc. Signal Process
Conference Date: 15-17 Feb. 1990 Conference Location: Sesimbra, Portugal
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: Inversion of multilayer synchronous networks is a method which tries to answer questions like 'What kind of input will give a desired output?' or 'Is it possible to get a desired (output under special input/output constraints)?'. The authors describe two methods of inverting a connectionist network. Firstly, they extend inversion via backpropagation to recurrent, time-delayed and discrete versions of continuous networks. The results of inversion is an input vector. The corresponding output vector is equal to the target vector except a small remainder. The knowledge of those attractors may help to understand the function and the generalization qualities of connectionist systems of this kind. Secondly, they introduce a new inversion method for proving the nonexistence of an input combination under special constraints, e.g. in a subspace of the input space. This method works by iterative exclusion of invalid activation values . It might be a helpful way to judge the properties of a trained network. They conclude with simulation results of three different tasks: XOR, morse signal decoding and handwritten digit recognition. (11 Refs)
Subfile: C

? t19/7/all

19/7/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

10477723
Title: Fractal analysis of yeast cell optical speckle
Author(s): Flamholz, A.; Schneider, P.S.; Subramaniam, R.; Wong, P.K.; Lieberman, D.H.; Cheung, T.D. ; Burgos, J.; Leon, K.; Romero, J.
Author Affiliation: Queensborough Community Coll., CUNY, Bayside, NY, USA
Journal: Proceedings of the SPIE - The International Society for Optical Engineering Conference Title: Proc. SPIE - Int. Soc. Opt. Eng. (USA) vol.6084, no.1 p.186-95
Publisher: SPIE-Int. Soc. Opt. Eng,
Publication Date: 2006 Country of Publication: USA
CODEN: PSISDG ISSN: 0277-786X

SICI: 0277-786X(2006)6084:1L.186:FAYC;1-H
Material Identity Number: C574-2006-041
Conference Title: Optical Interactions with Tissue and Cells XVII
Conference Date: 23 Jan. 2006 Conference Location: San Jose, CA, USA
DOI: 10.1117/12.646399
Language: English Document Type: Conference Paper (PA); Journal Paper (JP)
Treatment: Experimental (X)
Abstract: Steady state laser light propagation in diffuse media such as biological cells generally provide bulk parameter information, such as the mean free path and absorption, via the transmission profile. The accompanying optical speckle can be analyzed as a **random** spatial **data** series and its fractal dimension can be used to further classify biological media that show similar mean free path and absorption properties, such as those obtained from a single population. A population of yeast cells can be separated into different portions by centrifuge, and microscope analysis can be used to provide the population statistics. Fractal analysis of the speckle suggests that lower fractal dimension is associated with higher cell packing density. The spatial intensity correlation revealed that the higher cell packing gives rise to higher refractive index. A calibration sample system that behaves similar as the yeast samples in fractal dimension, spatial intensity correlation and diffusion was selected. Porous silicate slabs with different refractive index values controlled by water content were used for system calibration. The porous glass as well as the yeast **random** spatial **data** series fractal dimension was found to depend on the imaging resolution. The fractal method was also applied to fission yeast single cell fluorescent data as well as aging yeast optical data; and consistency was demonstrated. It is concluded that fractal analysis can be a high sensitivity tool for relative comparison of cell structure but that additional diffusion measurements are necessary for determining the optimal image resolution. Practical application to dental plaque bio-film and cam-pill endoscope images was also demonstrated. (15 Refs)
Subfile: A B

19/7/2 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

08736646 INSPEC Abstract Number: B2003-10-6220W-002
Title: **A 0.58-1 Gb/s CMOS data recovery circuit using a synchronous digital phase aligner**
Author(s): **Cheung, T.S. ; Lee, B.C.**
Author Affiliation: Dept. of Network Core Technol., ETRI, Daejon, South Korea
Conference Title: 2002 45th Midwest Symposium on Circuits and Systems. Conference Proceedings (Cat. No.02CH37378) Part vol.3 p.III-385-8 vol.3
Publisher: IEEE, Piscataway, NJ, USA
Publication Date: 2002 Country of Publication: USA 3 vol.(xlii+686+678+699) pp.
ISBN: 0 7803 7523 8 Material Identity Number: XX-2003-00384
U.S. Copyright Clearance Center Code: 0-7803-7523-8/02/$17.00
Conference Title: Midwest Symposium on Circuits and Systems
Conference Sponsor: IEEE Circuits & Syst. Soc.; School of Electr. & Comput. Eng. at Oklahoma State Univ
Conference Date: 4-7 Aug. 2002 Conference Location: Tulsa, OK, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: A data recovery circuit using a newly proposed synchronous digital phase aligner is realized for multi-link applications. The proposed circuit is implemented with 0.35 mu m CMOS process technology. The experimental results show that the proposed circuit successfully recovers

incoming 0.58-1 Gb/s of 2/sup 31/-1 pseudo random bit sequence with less than 10/sup -14/ of bit error rate. (5 Refs)
Subfile: B

?

Interference search

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L40	0	((encrypt$4) and (decrypt$4) and (original string) and (defin$4 set of factors) and (encrypt$4 equation) and (map$4) and (a set of derivative equations) and (generat$4 derivative values) and (stor$4 encrypted string and derivative values) and (provid$4 false derivatives cannot be used to determine a given factor) and (stor$4 false derivative values with the generated derivative values) and (us$4 a set of factor decryption equatins to map) and (decrypt$4 the encrypted string) and (decryption equation) and (factor mapped through the set of factor decryption equation) and (presence) and (false derivative values with the generated derivative values) and (prevent$4) and (use with the factor decryption equation to derive the factors in the set of facotrs)).clm.	US-PGPUB; USPAT	ADJ	ON	2007/10/11 22:17

NPL search

Terms used:
false derivative values not used to determine factor and **derivative values** and **encrypt** and **decrypt**

Found **124,412** of **212,128**

Sort results by: relevance
Display results: expanded form

Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Cryptography and data security
Dorothy Elizabeth Robling Denning
January 1982 Book
Publisher: Addison-Wesley Longman Publishing Co., Inc.
Full text available: pdf(19.47 MB) Additional Information: full citation, abstract, references, cited by, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

2 The relational model for database management: version 2
E. F. Codd
January 1990 Book
Publisher: Addison-Wesley Longman Publishing Co., Inc.
Full text available: pdf(28.61 MB) Additional Information: full citation, abstract, references, cited by, index terms, review

From the Preface (See Front Matter for full Preface)

An important adjunct to precision is a sound theoretical foundation. The relational model is solidly based on two parts of mathematics: firstorder predicate logic and the theory of relations. This book, however, does not dwell on the theoretical foundations, but rather on all the features of the relational model that I now perceive as important for database users, and therefore for DBMS vendors. My perceptions result from 20 y ...

3 On randomization in sequential and distributed algorithms
Rajiv Gupta, Scott A. Smolka, Shaji Bhaskar
March 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 1
Publisher: ACM Press

Full text available: pdf(8.01 MB) Additional Information: full citation, abstract, references, citings, index terms

Probabilistic, or randomized, algorithms are fast becoming as commonplace as conventional deterministic algorithms. This survey presents five techniques that have been widely used in the design of randomized algorithms. These techniques are illustrated using 12 randomized algorithms—both sequential and distributed— that span a wide range of applications, including:primality testing (a classical problem in number theory), interactive probabilistic proof s ...

Keywords: Byzantine agreement, CSP, analysis of algorithms, computational complexity, dining philosophers problem, distributed algorithms, graph isomorphism, hashing, interactive probabilistic proof systems, leader election, message routing, nearest-neighbors problem, perfect hashing, primality testing, probabilistic techniques, randomized or probabilistic algorithms, randomized quicksort, sequential algorithms, transitive tournaments, universal hashing

4 A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks

Radha Poovendran, Loukas Lazos
January 2007 **Wireless Networks**, Volume 13 Issue 1
Publisher: Kluwer Academic Publishers
Full text available: pdf(1.37 MB) Additional Information: full citation, abstract, references, index terms

Wireless ad hoc networks are envisioned to be randomly deployed in versatile and potentially hostile environments. Hence, providing secure and uninterrupted communication between the un-tethered network nodes becomes a critical problem. In this paper, we investigate the wormhole attack in wireless ad hoc networks, an attack that can disrupt vital network functions such as routing. In the wormhole attack, the adversary establishes a low-latency unidirectional or bi-directional link, such as a wir ...

Keywords: geometric random graphs, security, wireless ad hoc networks, wormhole attack

5 Technical reports

SIGACT News Staff
January 1980 **ACM SIGACT News**, Volume 12 Issue 1
Publisher: ACM Press
Full text available: pdf(5.28 MB) Additional Information: full citation

6 A survey of RST invariant image watermarking algorithms

Dong Zheng, Yan Liu, Jiying Zhao, Abdulmotaleb El Saddik
July 2007 **ACM Computing Surveys (CSUR)**, Volume 39 Issue 2
Publisher: ACM Press
Full text available: pdf(5.53 MB) Additional Information: full citation, abstract, references, index terms

In this article, we review the algorithms for rotation, scaling and translation (RST) invariant image watermarking. There are mainly two categories of RST invariant image watermarking algorithms. One is to rectify the RST transformed image before conducting watermark detection. Another is to embed and detect watermark in an RST invariant or semi-invariant domain. In order to help readers understand, we first introduce the fundamental theories and techniques used in the existing RST invariant ...

Keywords: Digital image watermarking, Fourier-Mellin transform, ILPM, LPM, RST invariant, Radon transform, feature points, moments, template matching

7 The internet worm program: an analysis

Eugene H. Spafford
January 1989 **ACM SIGCOMM Computer Communication Review**, Volume 19 Issue 1
Publisher: ACM Press
Full text available: pdf(2.45 MB) Additional Information: full citation, abstract, citings, index terms

On the evening of 2 November 1988, someone infected the Internet with a *worm* program. That program exploited flaws in utility programs in systems based on BSD-derived versions of UNIX. The flaws allowed the program to break into those machines and copy itself, thus *infecting* those systems. This program eventually spread to thousands of machines, and disrupted normal activities and Internet connectivity for many days.This report gives a detailed description of the components of the ...

8 An architecture for secure wide-area service discovery

Todd D. Hodes, Steven E. Czerwinski, Ben Y. Zhao, Anthony D. Joseph, Randy H. Katz
March 2002 **Wireless Networks**, Volume 8 Issue 2/3
Publisher: Kluwer Academic Publishers
Full text available: pdf(365.68 KB) Additional Information: full citation, abstract, references, citings, index terms

The widespread deployment of inexpensive communications technology, computational resources in the networking infrastructure, and network-enabled end devices poses an interesting problem for end users: how to locate a particular network service or device out of hundreds of thousands of accessible services and devices. This paper presents the architecture and implementation of a secure wide-area Service Discovery Service (SDS). Service providers use the SDS to advertise descriptions of available ...

Keywords: location services, name lookup, network protocols, service discovery

9 Security Mechanisms in High-Level Network Protocols

Victor L. Voydock, Stephen T. Kent
June 1983 **ACM Computing Surveys (CSUR)**, Volume 15 Issue 2
Publisher: ACM Press
Full text available: pdf(3.23 MB) Additional Information: full citation, references, citings

10 Magic Functions: In Memoriam: Bernard M. Dwork 1923--1998

Cynthia Dwork, Moni Naor, Omer Reingold, Larry Stockmeyer
November 2003 **Journal of the ACM (JACM)**, Volume 50 Issue 6
Publisher: ACM Press
Full text available: pdf(708.05 KB) Additional Information: full citation, abstract, references, citings, index terms

We prove that three apparently unrelated fundamental problems in distributed computing, cryptography, and complexity theory, are essentially the same problem. These three problems and brief descriptions of them follow. (1) *The selective decommitment problem.* An adversary is given commitments to a collection of messages, and the adversary can ask for some subset of the commitments to be opened. The question is whether seeing the decommitments to these open plaintexts allows the adversary t ...

Keywords: Digital signature, Fiat-Shamir methodology, interactive argument, interactive proof system, magic function, selective decommitment, zero knowledge

11 Succinct representation of flexible and privacy-preserving access rights
Marina Blanton, Mikhail Atallah
November 2006 **The VLDB Journal — The International Journal on Very Large Data Bases**, Volume 15 Issue 4
Publisher: Springer-Verlag New York, Inc.
Full text available: pdf(525.96 KB) Additional Information: full citation, abstract

We explore the problem of portable and flexible privacy preserving access rights that permit access to a large collection of digital goods. *Privacy-preserving* access control means that the service provider can neither learn what access rights a customer has nor link a request to access an item to a particular customer, thus maintaining privacy of both customer activity and customer access rights. *Flexible* access rights allow a customer to choose a subset of items or groups of items ...

Keywords: Compact representation, Flexible access rights, Privacy-preserving access rights

12 Paper session DB-10 (databases): query processing 2: Balancing performance and confidentiality in air index
Qingzhao Tan, Wang-Chien Lee, Baihua Zheng, Peng Liu, Dik Lun Lee
October 2005 **Proceedings of the 14th ACM international conference on Information and knowledge management CIKM '05**
Publisher: ACM Press
Full text available: pdf(320.99 KB) Additional Information: full citation, abstract, references, index terms

Studies on the performance issues (i.e., access latency and energy conservation) of wireless data broadcast have appeared in the literature. However, the important security issues have not been well addressed. This paper investigates the tradeoff between performance and security of signature-based air index schemes in wireless data broadcast. From the performance perspective, keeping low false drop probability helps clients retrieve the information from a broadcast channel efficiently. Meanwhile ...

Keywords: indexing techniques, security, wireless data broadcast

13 Symmetric and Asymmetric Encryption
Gustavus J. Simmons
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
Publisher: ACM Press
Full text available: pdf(2.23 MB) Additional Information: full citation, references, citings, index terms

14 Credentials: Concealing complex policies with hidden credentials
Robert W. Bradshaw, Jason E. Holt, Kent E. Seamons
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security CCS '04**
Publisher: ACM Press
Full text available: pdf(219.13 KB) Additional Information: full citation, abstract, references, citings, index terms

Hidden credentials are useful in protecting sensitive resource requests, resources, policies,

and credentials. We propose a significant performance improvement when implementing hidden credentials using Boneh/Franklin Identity Based Encryption. We also propose a substantially improved secret splitting scheme for enforcing complex policies, and show how it improves concealment of policies from nonsatisfying recipients.

Keywords: authentication, credentials, identity based encryption, privacy, secret sharing, trust negotiation

15 Applying hierarchical and role-based access control to XML documents

Jason Crampton

October 2004 **Proceedings of the 2004 workshop on Secure web service SWS '04**

Publisher: ACM Press

Full text available: pdf(337.19 KB) Additional Information: full citation, abstract, references, citings, index terms

W3C Recommendations XML Encryption and XML-Digital Signature can be used to protect the confidentiality of and provide assurances about the integrity of XML documents transmitted over an insecure medium. The focus of this paper is how to control access to XML documents, once they have been received. This is particularly important for services where updates are sent to subscribers. We describe how certain access control policies for restricting access to XML documents can be enforced by encryptin ...

Keywords: XML, encryption, hierarchical access control, role-based access control

16 The security of all RSA and discrete log bits

Johan Håstad, Mats Näslund

March 2004 **Journal of the ACM (JACM)**, Volume 51 Issue 2

Publisher: ACM Press

Full text available: pdf(311.91 KB) Additional Information: full citation, abstract, references, index terms

We study the security of individual bits in an RSA encrypted message $E_N(x)$. We show that given $E_N(x)$, predicting any single bit in x with only a nonnegligible advantage over the trivial guessing strategy, is (through a polynomial-time reduction) as hard as breaking RSA. Moreover, we prove that blocks of $O(\log \log N)$ bits of x are computationally indistinguishable from random bits. The results carry over t ...

Keywords: Cryptography, RSA-encryption, bit-security, complexity, discrete logarithms

17 New basic technologies for DIM: Pseudonym management using mediated identity-based cryptography

Thibault Candebat, Cameron Ross Dunne, David T. Gray

November 2005 **Proceedings of the 2005 workshop on Digital identity management DIM '05**

Publisher: ACM Press

Full text available: pdf(293.16 KB) Additional Information: full citation, abstract, references, index terms

Mobile Location-Based Services (LBS) have raised privacy concerns amongst mobile phone users who may need to supply their identity and location information to untrustworthy third parties in order to access these applications. Widespread acceptance of such services may therefore depend on how privacy sensitive information will be handled in order to restore users' confidence in what could become the "killer app" of 3G networks. In this

paper, we present a proxy-based public key infrastructure tha ...

Keywords: SEM architecture, identity-based encryption, location-based services, pseudonymity

18 A fuzzy commitment scheme

Ari Juels, Martin Wattenberg

November 1999 **Proceedings of the 6th ACM conference on Computer and communications security CCS '99**

Publisher: ACM Press

Full text available: pdf(966.08 KB) Additional Information: full citation, abstract, references, citings, index terms

We combine well-known techniques from the areas of error-correcting codes and cryptography to achieve a new type of cryptographic primitive that we refer to as a fuzzy commitment scheme. Like a conventional cryptographic commitment scheme, our fuzzy commitment scheme is both concealing and binding: it is infeasible for an attacker to learn the committed value, and also for the committer to decommit a value in more than one way. In a convent ...

19 Security and correctness: Efficient data protection for distributed shared memory multiprocessors

Brian Rogers, Milos Prvulovic, Yan Solihin

September 2006 **Proceedings of the 15th international conference on Parallel architectures and compilation techniques PACT '06**

Publisher: ACM Press

Full text available: pdf(386.29 KB) Additional Information: full citation, abstract, references, index terms

Data security in computer systems has recently become an increasing concern, and hardware-based attacks have emerged. As a result, researchers have investigated hardware encryption and authentication mechanisms as a means of addressing this security concern. Unfortunately, no such techniques have been investigated for Distributed Shared Memory (DSM) multiprocessors, and previously proposed techniques for uni-processor and Symmetric Multiprocessor (SMP) systems cannot be directly used for DSMs. T ...

Keywords: DSM multiprocessor, data security, memory encryption and authentication

20 Software protection and simulation on oblivious RAMs

Oded Goldreich, Rafail Ostrovsky

May 1996 **Journal of the ACM (JACM)**, Volume 43 Issue 3

Publisher: ACM Press

Full text available: pdf(3.44 MB) Additional Information: full citation, abstract, references, citings, index terms

Software protection is one of the most important issues concerning computer practice. There exist many heuristics and ad-hoc methods for protection, but the problem as a whole has not received the theoretical treatment it deserves. In this paper, we provide theoretical treatment of software protection. We reduce the problem of software protection to the problem of efficient simulation on oblivious RAM.A machine is oblivious if thhe sequence in wh ...

Keywords: pseudorandom functions, simulation of random access machines, software protection

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next